| COMSCINST 5239.3 | COG CODE N6 | DATE 22 OCT 1992 |
|---|---|---|

**DEPARTMENT OF THE NAVY**
COMMANDER MILITARY SEALIFT COMMAND
WASHINGTON NAVY YARD BLDG 210
901 M STREET SE
WASHINGTON DC 20398-5540

COMSCINST 5239.3
N6
22 October 1992

COMSC INSTRUCTION 5239.3

Subj: AUTOMATED INFORMATION SYSTEMS (AIS) SECURITY PLAN (AISSP)

Ref: (a) SECNAVINST 5239.2
(b) OPNAVINST 5239.1A
(c) DOD Directive 5200.28 of 21 Mar 88

Encl: (1) MSC AIS Security Plan (AISSP)

1. Purpose. To establish MSC AIS Security Program and promulgate enclosure (1). Enclosure (1) is a complete revision and should be reviewed in its entirety.

2. Background. References (a) and (b) provide DON policy and procedures for AIS Security Program. MSC implementation is set forth in enclosure (1).

3. Action. MSC Directors and Special Assistants will review enclosure (1) and ensure staff compliance. The Command, Control, Communication and Computer (C4) Systems Director (N6) is delegated authority to sponsor all networks and AISs and administer enclosure (1) and ensure compliance with references (a) through (c). Specific responsibilities are detailed in Chapter 2 of enclosure (1), which refers to delegated authority where applicable.

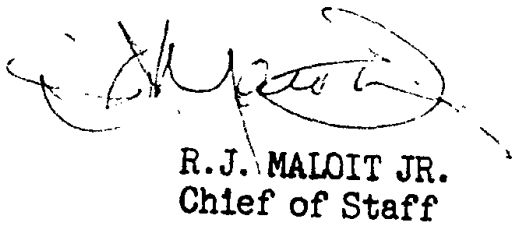
a. COMSC is Designated Approving Authority (DAA) for AIS and is responsible for providing adequate security to protect MSC AIS resources.

b. Directors and Special Assistants are responsible for AIS Security of AIS systems used within their cognizant area, including nominating Terminal Area Security Officers (TASOs) to N6.

c. Project Managers are responsible for AIS Security of their AIS projects, including obtaining an interim authority to operate or accreditation prior to implementation.

d. User Sponsors are responsible for ensuring AIS security issues are addressed prior to implementation of AIS systems within their cognizance area.

e. Individual users are responsible for operating AIS systems within guidelines of enclosure (1) and for reporting security violations.



R.J. MALOIT JR.
Chief of Staff

Distribution:
COMSCINST 5000.19
List I (Case A, B)
List II (Case A, B)

# TABLE OF CONTENTS

**CHAPTER** **PAGE**

**1 MILITARY SEALIFT COMMAND AUTOMATED INFORMATION SYSTEMS SECURITY PLAN (AISSP)**

1.1 General ..... 1-1
1.2 Policy ..... 1-1
1.3 Scope ..... 1-3
1.4 Objectives ..... 1-4
1.5 Classified Information Processing Systems ..... 1-5
1.6 Definitions and Acronyms ..... 1-5

**2 ORGANIZATION AND RESPONSIBILITIES**

2.1 AIS Security Organization ..... 2-1
2.2 Responsibilities ..... 2-1
2.2.1 Commander, Military Sealift Command ..... 2-1
2.2.2 MSC Directors/Special Assistants ..... 2-1
2.2.3 MSC Security Officer ..... 2-2
2.2.4 AIS Project Managers ..... 2-2
2.2.5 MSC AIS Security Staff ..... 2-3
2.2.5.1 ADP Security Officer ..... 2-3
2.2.5.2 ADP Network Security Officer ..... 2-5
2.2.5.3 ADP System Security Officer ..... 2-5
2.2.5.4 Terminal Area Security Officer ..... 2-7
2.2.6 MSC Functional Sponsors ..... 2-8
2.2.7 Individual Users ..... 2-9
2.2.8 Contracting Officers ..... 2-9
2.2.9 Contractors ..... 2-10
2.3 AIS Security Staff Requirements ..... 2-10
2.3.1 ADP Security Officer ..... 2-10
2.3.2 ADP Network Security Officer ..... 2-10
2.3.3 ADP System Security Officer ..... 2-11
2.3.4 Terminal Area Security Officer ..... 2-11

**3 COMSC AUTOMATED INFORMATION SYSTEMS SECURITY ENVIRONMENT**

3.1 AIS Security Environment ..... 3-1
3.2 Hardware ..... 3-1
3.3 Software ..... 3-1
3.4 Physical Facility/Security ..... 3-1
3.5 Personnel ..... 3-2
3.6 Communications ..... 3-2
3.7 Emanations ..... 3-2
3.8 Administrative/operating Procedures ..... 3-2
3.9 Data ..... 3-2

**4 AUTOMATED INFORMATION SYSTEMS SECURITY TRAINING**

4.1 Introduction ..... 4-1
4.2 Training Policy 4-1
4.3 AIS Security Curriculum ..... 4-2
4.4 AIS Security Staff ..... 4-2

**5 AUDIT AND INTERNAL REVIEW**

5.1 Internal Review Schedule and Team Membership ..... 5-1
5.2 Compliance Responsibility ..... 5-1
5.3 Components of the Security Review ..... 5-1
5.4 Security Incident Reports ..... 5-1
5.5 Fraud, Waste and Abuse Actions ..... 5-2

**6 LIFE CYCLE MANAGEMENT (LCM)**

6.1 LCM security Requirements ..... 6-1
6.2 AIS Project Manager LCM Responsibilities ..... 6-1
6.3 Classified and Sensitive Data ..... 6-1
6.4 Risk Index 6-1

**7 CONFIGURATION MANAGEMENT**

7.1 Configuration Management ..... 7-1

**8 CONTINGENCY PLANNING**

8.1 Contingency Plans ..... 8-1
8.2 Mandatory Procedures ..... 8-1
8.3 Scope of the Contingency Plan ..... 8-1
8.4 General Guidance ..... 8-1

**9 ACCREDITATION AND CERTIFICATION**

9.1 Accreditation Requirements ..... 9-1
9.2 HSC Accreditation ..... 9-2
9.3 Project Accreditation or Certification ..... 9-2
9.3.1 Project Accreditation Where COMSC Is DAA ..... 9-2
9.3.2 Project Accreditation Where COMSC Is Not DAA ..... 9-2
9.3.3 Project Certification ..... 9-3
9.4 Interim Authority to Operate ..... 9-3

**APPENDICES**


| | | |
|---|---|---|
| A | Part I - Definitions | A-1 |
| | Part II - Acronyms | A-12 |
| B | Bibliography | B-1 |
| C | DOD and DON AIS Security Policies | C-I |
| D | Security of AIS Media | D-I |
| E | Security Guidance for Workstations | E-I |
| F | Risk Assessment | F-1 |
| G | Security Test and Evaluation (ST&E) | G-1 |
| H | Mandatory Minimum Requirements | H-1 |
| I | Accreditation Support Documentation | I-1 |
| J | Project Accreditation and Certification | J-1 |

# CHAPTER 1

## MILITARY SEALIFT COMMAND AUTOMATED INFORMATION SYSTEMS SECURITY PLAN (AISSP)

**1.1 GENERAL.** The Military Sealift Command (MSC) Automated Information Systems (AIS) Security Plan (AISSP) promulgates DOD, NAVY and MSC AIS security policy and provides guidelines for AIS security procedures to be used by MSC Headquarters. AIS functions are set forth in COMSCINST 5223.1B, Information Resource Management Program, and are under the Command, Control, Communication and Computer Systems Directorate (C4S). This plan documents current MSC Headquarters AIS security environment, establishes program objectives and outlines a plan of action and milestones for activity accreditation.

a. The acronym AIS is used extensively throughout this plan to designate the full range of information and computer system services, including office information systems and networks. MSC AIS encompasses all Automated Data Processing (ADP) resources, computer resources, information system development projects, office information systems and information system networks. To maintain consistency with current DON usage, the acronyms ADPSO, ADPSSO and ADPNSO are used in this plan to connote Automated Data Processing Security Officer, Automated Data Processing System Security Officer and Automated Data Processing Network Security Officer.

b. The AISSP establishes MSC AIS security policies, defines the scope and objectives of these policies and assigns responsibilities. The AISSP is the first of three parts in the MSC AIS risk management program. MSC AIS risk management program includes:

(1) Maintenance of the AISSP.

(2) Periodic risk assessments.

(3) Countermeasures and effectiveness reviews, in the form of System Test and Evaluations (ST&Es).

**1.2 POLICY.** It is the policy of Commander, Military Sealift Command (COMSC), that MSC AIS resources be operated in compliance with OPNAVINST 5239.1A and other applicable security directives.

a. MSC AIS resources will be operated only when the following criteria are satisfied:

(1) The system is accredited; or an interim authority to operate has been granted in writing by the Commander, Military Sealift Command, in his capacity as Designated Approving Authority (DAA); and

(2) TEMPEST requirements of OPNAVINST C5510.93E have been satisfied for systems processing Level I data; and

(3) All Level I Top Secret material is only processed in system high or dedicated security mode; and

(4) All Level I Secret or Confidential material is only processed in system high, dedicated or controlled security mode; and

(5) For equipment connected to World Wide Military Command and Control System (WWMCCS), approval has been granted by WWMCCS System Security Office (WASSO).

b. Currently MSC does not process any classified material meeting following criteria, and thus special requirements for such are not covered in this AISSP. If MSC should have need to process classified material meeting any of the following criteria, this AISSP will be updated.

(1) Level I SCI material.

(2) Single Integrated Operational Plan - Extremely Sensitive Information (SIOP-ESI).

(3) Top Secret, Secret or Confidential material in a multilevel or controlled mode.

(4) Level I National Cryptologic material, except as may be included as part of World Wide Military Command and Control System (WWMCCS).

c. Employees and contractors will adhere to following rules for operation of personally owned microcomputers:

(1) Privately owned personal computers will not be used or connected to an MSC computer, or network, without the written consent of the Commander, Military Sealift Command, in his capacity as Designated Approving Authority (DAA), or his delegated authority, ADPSO.

(2) Classified data will not be processed on any privately owned computer system, without written consent of the DAA, or his delegated authority, ADPSO.

d. An MSC AIS security survey will be completed for all new AIS resources prior to procurement or development. This survey is to part of the Life Cycle Management Process (LCM) as detailed in Chapter 6. Based on the responses contained in the survey, MSC ADP Security Officer (ADPSO), or designated ADP System security Officer (ADPSSO), will identify safeguards and accreditation documentation necessary.

e. The MSC AIS security program has been established in accordance with OPNAVINST 5239.1A. This program is under the Command, Control, Communication and Computer (C4) Systems Director (N6) and includes risk assessments, Security Test and Evaluations (ST&E) and contingency planning. This AISSP documents AIS security program and is maintained by ADPSO. AISSP updates will be made upon any major changes to MSC AIS or other factors that affect AISSP integrity.

f. Specific security concerns of shipboard systems are addressed in the Shipboard Management Information System (SMIS) Security Plan. Development, maintenance and use of systems designed for shipboard use will comply with both the contents of this plan and the SMIS Security Plan. SMIS Security Plan maintenance is provided by Director, Afloat Shipboard Systems Division, N64.

g. Contractor assistance will not be obtained in conducting a risk assessment, an ST&E or a contingency test before formally requesting technical assistance from the Commander, Naval Data Automation Command (COMNAVDAC).

h. DOD and DON AIS security policies from OPNAVINST 5239.1A are provided in Appendix C.

**1.3 SCOPE.** The AISSP for MSC serves as a central planning and management tool in controlling the AIS security environment. The plan applies to all AIS resources, IS networks and local area networks (LANs) in use within MSC Headquarters including, but not limited to, the following:

a. The term workstations refers to any electronic device capable of storing in memory or on any media any form of data, instructions or programs and any electronic device used to communicate with a host computer of any size. This includes, but is not limited to microcomputers, intelligent and dumb terminals, memory typewriters, word processors and Office Information Systems (OIS). The single exception is programmable, hand held calculators for which no means exists with which data or programs can be exchanged from one to another hand held calculator.

b. Minicomputers and mainframes, should they be obtained or operated by MSC.

c. Non-Government owned/leased personal computers that access AIS resources controlled or paid for by the government even if such access is from a non-Government controlled workspace (i.e., home) and non-Government owned/leased computers brought into a Government controlled workspace.

d. Processing by contractors using MSC owned or controlled equipment.

e. Contractor owned resources within government spaces for which MSC is the Contracting Officer's Technical Representative (COTR).

f. Processing of MSC controlled data using contractor owned equipment.

g. All shoreside installations of support systems to the Shipboard Management Information Systems (SMIS).

**1.4 OBJECTIVES.** Objectives of this plan are to meet all requirements of the Department of Navy AIS Security Program as promulgated in OPNAVINST 5239.1A including:

a. Provide centralized policy guidance for AIS Security as it applies to MSC 5 headquarters and Area Commands environment.

b. Provide generalized procedures and guidance to ensure that equipment and software associated with the AIS environment is protected to maximum practical extent against modification, destruction, disclosure or denial of service. The goal is to minimize those impacts whether through inadvertent or intentional acts, mishap, misappropriation or natural acts.

c. Provide centralized guidance and uniform policy on AIS security to responsible personnel.

d. Provide guidelines and procedures to ensure that all classified and sensitive information handled by automated systems is protected against threats at a level consistent with value of the system or data.

e. Provide for operational reliability and asset integrity of all information systems and telecommunications networks through a structured program of AIS security.

f. Safeguard classified information through continuous employment of protective countermeasures designed to ensure integrity of AIS databases and operating environments.

g. Establish and maintain a formal risk management program to assist in identifying threats, vulnerabilities, countermeasures and contingency plans to control risks.

h. Ensure the establishment and maintenance of formal AIS accreditation.

i. Provide for development of adequate contingency plans to provide for the continuity of operations in the event a system is damaged, destroyed or compromised.

j. Include AIS security requirements in the acquisition of all new AIS resources.

**1.5 CLASSIFIED INFORMATION PROCESSING SYSTEMS.** It is to be noted that this AISSP does not automatically apply to equipment referred to as Classified Information Processing Systems (CLIPS) by OPNAVINST C5510.93E. OPNAVINST C5510.93E, Navy Implementation of National Policy on Control of Compromising Emanations, applies to devices that may emit compromising emanations. This includes such things as electric typewriters, such as the IBM Selectric, and photo-copying equipment. The term CLIPS, as defined by OPNAVINST C5510.93E, includes all equipment covered by this AISSP as well as equipment beyond the scope of this plan.

**1.5.1** MSC has appointed a TEMPEST Control Officer (TCO) as required by OPNAVINST C5510.93E. The TCO maintains copies of TEMPEST vulnerability Requests (TVARs) and the resulting Instrumented TEMPEST Surveys (ITSs). Together, the TVARs and ITSs provide a record of the authorized CLIPS, some of which are subject to this AISSP.

**1.6 DEFINITIONS AND ACRONYMS.** Appendix A provides a glossary of terms and acronyms. All terms are used as defined in Appendix A.

# CHAPTER 2

# ORGANIZATION AND RESPONSIBILITIES

**2.1 AIS SECURITY ORGANIZATION.** The MSC AIS security organization is obtained through assignment of collateral duties and responsibilities inherent with specific positions. There are no full time positions assigned solely to AIS security duties at MSC Headquarters.

## 2.2 RESPONSIBILITIES

**2.2.1** Commander, Military Sealift Command is responsible for:

a. Maintaining an AIS security Plan (AISSP) so as to provide adequate security to protect MSC AIS resources (i.e., activities, AIS networks and Office Information Systems (OIS)), including the integrity of data being handled.

b. Performing as Designated Approving Authority (DAA).

c. Appointing an ADP Security Officer (ADPSO) in writing to act as the focal point for all MSC AIS security matters.

d. Appointing an ADPNSO in writing for MSC networks.

e. Ensuring that contract specifications for AIS equipment, software, maintenance services, professional or other services or supplies satisfy AIS security requirements.

f. Ensuring that security requirements are included in Life Cycle Management (LCM) documentation as prescribed in SECNAVINSTs 5000.lC (NOTAL) or 5231.lC (NOTAL) as appropriate.

**2.2.2** Directors/Special Assistants are responsible for:

a. Ensuring staff compliance with all security guidelines, regulations, directives, notices and this AISSP.

b. Nomination of staff to assume collateral AIS security duties as required by this AISSP.

c. Ensuring that AIS related security violations are documented in writing and reported to MSC Security Officer and ADPSO in a timely manner.

d. Ensuring that access to AIS equipment, data and software is limited to authorized personnel.

e. Ensuring that AIS security is included in all staff members' training plans.

f. Ensuring that new personnel are trained in AIS security.

g. Ensuring that all staff participate in periodic security awareness training as required by Public Law 100-235, Computer Security Act of 1987, 8 January 1988.

h. Informing the ADPSO of AIS security training and attendance at such training.

i. Assigning the classified/sensitive-unclassified/ unclassified label to data for those data elements originated by or through their directorate.

j. Acting as Terminal Area Security Officer (TASO) for their office spaces if one has not been assigned.

**2.2.3** The Command Security Officer is responsible for coordinating with ADPSO on matters relating to AIS security.

**2.2.4** AIS Project Managers are responsible for:

a. Ensuring that when an AIS is or will be run at multiple activities or sites, operating system and application software has been certified for multisite distribution.

b. Ensuring that security concerns are addressed in the network under their cognizance.

c. Ensuring that security concerns are addressed as part of Life Cycle Management (LCM) process as specified in Chapter 6 of this AISSP.

d. Ensuring that training includes coverage of security.

e. Preparation, documentation, testing and evaluation of contingency plans as specified in Chapter 8 of this AISSP.

f. Obtaining an interim authority to operate or accreditation prior to operating an AIS.

g. Obtaining and maintenance of accreditation or certification, as outlined in Chapter 9, for the entire life cycle.

h. Acting as ADPSSO if one is not appointed.

i. Ensuring that TEMPEST requirements for processing classified data are identified at the earliest stages of the development process and that no such systems are operated until proper TEMPEST requirements have been satisfied.

j. Ensuring that security requirements for processing classified and sensitive unclassified data are identified, planned for and maintained at the earliest possible phase of the LCM process.

k. Ensuring that classified and sensitive unclassified data are not accessible from off site locations unless the commanding officer/DAA or ADPSO certify that the AIS adequately protects such data and that such off site use will not violate applicable strictures within this instruction. Such data, when stored on electronic media, should not be removed from MSC spaces without proper approval from DAA or delegated authority. This approval should:

(1) Identify data by types of record, specific records and file name, if practicable;

(2) Specify what data may not be created, accessed or taken off site;

(3) Specify what data may be created, accessed or taken off site, subject to stated controls;

(4) Specify what data may be created, accessed or taken off site at the discretion of the employee and supervisor;

(5) Specify a check-out procedure for electromagnetic media;

(6) Require that a backup copy be retained in the office.

l. Ensuring that AIS acquisition planning gives due consideration to the security and integrity of MSC data and conformance with software license terms.

m. Ensuring compliance with this AISSP, OPNAVINST 5239.1A and DOD Directive 5200.28 at all times.

n. Notifying N6 and the ADPSO in writing of the relative apportionment of classified/sensitive-unclassified/unclassified data associated with each project prior to the start at design work. Written notice will be made of any changes in this relative apportionment as soon as the change is known.

**2.2.5** MSC AIS Security Staff The AIS Security Staff is responsible for ensuring implementation and adherence to this AISSP within their assigned areas. To enable the staff to execute their responsibilities they are to be trained, by formal education or self study, as required to satisfy paragraph 4.4.

**2.2.5.1**The Automated Data Processing Security Officer (ADPSO) is responsible for:

a. Coordinating with Command Security Officer on matters concerning AIS security, in accordance with the security directives established by COMSC and OPNAVINST 5510.1H.

(1) ADPSO is responsible to Command Security Officer for the protection of classified information being processed in AIS.

(2) ADPSO is responsible to the Command Physical security Officer for the protection of the personnel, equipment and related resources used in AIS.

b. Ensuring that an Automated Information Systems security Plan (AISSP) is developed and maintained.

c. Ensuring that an ADPNSO is appointed for MSC networks.

d. Ensuring that ADPSSOs are appointed in writing.

e. Ensuring that a Terminal Area Security Officer (TASO) is appointed for each workstation or cluster of workstations and associated devices.

f. Ensuring that an effective activity Risk Management Program is implemented.

g. Ensuring that requests for accreditation of AIS activities and networks are completed in accordance with this AISSP.

h. Ensuring that all AIS security incidents or violations are investigated, documented and reported. Copies of these incident reports should be provided to the ADPSSO and forwarded to NAVCOMTELCOM.

i. Ensuring that security requirements are included in Life Cycle Management (LCM) documentation as prescribed in SECNAVINSTs 5000.lC (NOTAL) or 5231.lC (NOTAL) as appropriate.

j. Ensuring that all procurement documents or specifications under consideration prior to approval by COMSC, comply with appropriate AIS security requirements as identified in paragraph 2.2.8.

k. Ensuring the development and testing of all contingency plans.

1. Ensuring that accreditation support documentation is developed and maintained.

m. Assisting the AIS security staff in implementing their respective AIS security responsibilities.

n. Ensuring that applicable personnel security procedures are established for all AIS activities and networks.

o. Ensuring that a System Test and Evaluation (ST&E) is conducted as required by Appendix G of this AISSP.

p. Developing a COMSC Risk Assessment Team Charter and Plan of Action and Milestones (POA&M) when required to complete a Risk Assessment.

q. Maintaining a list of projects processing classified and sensitive unclassified data.

r. Assuming the AIS security staff responsibilities for any staff member not appointed.

s. Developing and maintaining an AIS security training program, including maintaining a record of AIS security training.

**2.2.5.2**The Automated Data Processing Network Security Officer (ADPNSO) is responsible for:

a. Ensuring that countermeasures and requirements are included in network design and that individual nodes of the network comply with these countermeasures and requirements prior to interfacing with the network. The security requirements will be agreed to in writing by network DAA and COMSC, and implemented before node is connected to the network. Networks having multiple service/agency members will be accredited jointly. Network accreditation will be based on prior accreditation of each network node.

b. Developing and promulgating standard security procedures governing network operations.

c. Ensuring that security measures and procedures used at network nodes fully support security integrity of the network.

d. Maintaining liaison with all ADPSSOs in the network.

e. Ensuring that all required countermeasures are utilized.

f. Maintaining a list of all nodes, with ADPSSO, in the network.

g. Maintaining a list of all users of the network and administer password or other protection suitable for purpose of the network.

**2.2.5.3**An ADP System Security Officer (ADPSSO) will be appointed by the applicable N6 project manager for each AIS processing or planning to process classified or sensitive unclassified data. N6 or applicable N6 project manager may appoint an ADPSSO for an AIS processing unclassified data. Two or more AISs may have the same ADPSSO. For Information Systems under their cognizance, ADPSSOs will execute an AIS security program which is consistent with the intent of OPNAVINST 5239.1A, and COMSC instructions and is responsive to unique command operational requirements. ADPSSO will:

a. Be the focal point for all security matters for assigned AIS.

b. Execute AIS security program as it applies to assigned AIS including preparing and submitting accreditation support documentation.

c. Maintain an inventory of all hardware, implemented system software releases and major functional application systems (e.g., finance, personnel, logistics, etc.) for AIS.

d. Monitor system activity, including identification of levels and types of data handled by the AIS, assignment of passwords and review of audit trails, outputs, etc., to ensure compliance with security directives and procedures.

e. Maintain liaison with remote facilities served by AIS to ensure compliance with applicable security requirements.

f. Maintain liaison with remote facilities served by AIS to ensure that a Terminal Area Security Officer (TASO) is designated by served activity where applicable.

g. Conduct and document a risk assessment in accordance with Appendix F and directions of the ADPSO.

h. Develop a Systems Test and Evaluation (ST&E) plan, conduct an ST&E and document results.

i. Contribute to MSC AIS Security Plan with regard to assigned AIS.

j. Maintain accreditation or certification documentation for use in reaccreditation and satisfying audits.

k. Supervise, test and monitor, as appropriate, changes in AIS systems affecting the AIS activity and AIS network security posture.

1. Implement appropriate countermeasures required by directive or determined to be cost effective.

m. Assist the ADPSO in implementing a comprehensive MSC AIS security Program.

n. Develop and test annually all contingency plans as specified in Chapter 8.

o. Maintaining a list of all users and administer suitable access controls.

p. Monitor AIS procurements for security impact to ensure compliance with security regulations and known security requirements for assigned AIS.

q. Providing all users and applicable TASOs with annual reviews (i.e., training sessions) on AIS security as it relates to their systems.

r. Assisting the ADPSO with AIS security training.

**2.2.5.4**Terminal Area Security Officers (TASOs) will be appointed where applicable by any office, division or other grouping of personnel receiving AIS support. They will enforce all security requirements implemented by the ADPSSO/ADPSO for remote terminal areas. TASOs will ensure that all countermeasures required to protect remote areas are in place. TASOs shall:

a. Assist ADPSO and applicable ADPSSOs in preparing Terminal Area Security procedures for all assigned workstations.

b. Implement approved security procedures for all assigned workstations.

c. Maintain a current list of all AISs accessed by each assigned workstation, including the ADPSSO for each AIS.

d. Ensure that all microcomputers, printers, or workstations are labeled and are controlled at the highest classification of data authorized to be processed. The label will be visible to the operator and not easily removed.

e. Maintain a current list of all workstations and individual(s) who make regular use of each workstation.

f. Assist N6 in maintaining MSC inventory of AIS hardware and software resident in an automated database.

g. Ensure that all actual, or suspected, AIS security incidents or violations are investigated, documented and reported to management, the ADPSO and applicable ADPSSO.

h. Periodically inspect assigned workstations to determine extent that MSC property is safeguarded from unauthorized use and return any unclaimed or suspicious hardware or software to N6.

i. Be familiar with MSC AIS Security Program, applicable directives related to AIS security. Ensure that all new workstation users and operators are briefed on the proper security procedures for operation of the workstation.

j. Assist the ADPSO and ADPSSOs in conducting and documenting the AIS Security Accreditation, including Risk Assessment, Security Test and Evaluation and Contingency Planning.

k. Providing introductory AIS security training for all new personnel.

1. Assisting applicable ADPSSOs with annual training on AIS security as it relates to systems used in their area.

m. Assisting the ADPSO with AIS security training.

**2.2.6** MSC Functional Sponsors (FSs) will ensure that development personnel are aware of necessity for addressing AIS security issues at each stage of the development process. FS will:

a. Ensure that AIS security issues are addressed prior to implementation of major modifications or changes to their systems.

b. Ensure that AIS security requirements are incorporated in any Request for Proposal(s) or tasking statement issued for their systems.

c. Ensure that their representatives on system development teams have received training in AIS security.

d. Ensure that TEMPEST requirements for processing classified data are identified at earliest stages of development process and that no such systems are operated until the proper TEMPEST requirements have been satisfied.

e. Ensuring that N6 and the ADPSO are notified in writing of the relative proportions of classified/sensitive-unclassified/ unclassified data to be processed.

f. Ensure that security requirements for processing classified and sensitive-unclassified data are identified, planned for and maintained at earliest possible phase of LCM process.

g. Determining requirement for a contingency plan and making related recommendations to DAA as specified in Chapter 8 of this AISSP.

h. Ensure that accreditation or certification is obtained and maintained as specified in Chapter 9.

i. Ensure that AIS security is included in training provided to users.

**2.2.7** Individual users are first line of defense in any security effort. Users are responsible for:

a. Informing AIS management staff, AIS operations staff and the AIS security staff of the levels and types of data they require to be processed.

b. Processing only levels of data authorized for their particular system. Processing of classified data requires compliance with TEMPEST and regular security requirements.

c. Ensuring that security violations are reported to their supervisors, cognizant ADPSSO and TASO.

d. Adherence to all applicable physical and AIS security policies, procedures and regulations when operating their systems.

e. Notifying system's ADPSSO and TASO of any unexpected changes in system.

f. Operating systems for Official Navy business only.

g. Enforcement of all local security rules and regulations.

h. Compliance with Appendix E, Security Guidance for Workstations.

i. Attending, on an annual basis, at least one training session that covers AIS security.

**2.2.8** Contracting Officers and their representatives are responsible for:

a. Including a requirement for compliance with OPNAVINST 5239. 1A, and this AISSP in any contract dealing with AIS resources.

b. Including a requirement for compliance with OPNAVINST C5510.93E for all contracts involving the processing of classified data.

c. Ensuring that evaluation of all contractor proposals, bids, deliverables and other contractor items includes consideration of AIS security.

d. Notify contractors that they are responsible for Contractor Induced Computer Viruses (CICVs), or other malicious software, and that liability will be addressed under procurement regulations.

e. Require proposals to identify the methodology for preventing CICVs and other malicious software from being delivered to MSC.

f. Negotiate inspection and acceptance test clauses, CICV and other malicious software free warranties.

**2.2.9** Contractors doing business with MSC are responsible for:

a. Identification, implementation and maintenance of all applicable AIS security safeguards.

b. Familiarity with applicable government AIS security directives and Federal Information Processing Standards (FIPS).

c. Providing deliverables that are free of CICVs and other malicious software.

## 2.3 AIS SECURITY STAFF REQUIREMENTS

**2.3.1** ADP Security Officer has following requirements:

a. Organizational placement of position is at the discretion of COMSC.

b. A strong technical background and experience in administration of AIS and networks and an innovative ability in dealing with complex problems.

c. Technically qualified to develop and implement MSC AIS security program in accordance with DON AIS security Program.

d. As a minimum, qualifications specified for ADPSSO in paragraph 2.3.3. Generally, the ADPSO will have served as an ADPSSO prior to assuming ADPSO position.

e. Possession of a security clearance for highest level of classified information processed by MSC.

**2.3.2** ADP Network Security Officer has following requirements:

a. Technically qualified to implement AIS network security policies, standards and procedures and to resolve conflicts between nodes of network.

b. As a minimum, qualifications specified for ADPSSO in paragraph 2.3.3.

c. A strong technical background in teleprocessing and network concepts, network protocols, network interfaces between AIS hardware and software and communication circuits.

d. Possession of a security clearance far highest level of classified information processed on the network.

**2.3.3** ADP System security Officer has following requirements:

a. Technically qualified to execute the MSC AIS security program as it pertains to assigned AIS.

b. A strong technical background in AIS administration and technical experience in either computer operations, system software or application software. A minimum of 12 months experience is recommended.

c. Completion of professional training related to AIS security. Such training includes: general AIS security, Privacy Act of 1974, information security, physical security and hardware/software security techniques.

d. Completion of training related to an activity's particular AIS. Such training includes: operating systems analysis, hardware architecture, computer performance evaluation and teleprocessing and network concepts and operations.

e. Knowledge of application and enforcement of physical, personnel, emanations and administrative security countermeasures is necessary and highly recommended.

f. Possession of a security clearance for highest level of classified information to be processed.

**2.3.4** Terminal Area Security Officer has following requirements:

a. Technically qualified to ensure that AIS security policies and procedures applicable to the workstation or remote terminal area are followed and that all users have been indoctrinated concerning their security responsibilities.

b. Basic knowledge of computer technology used in assigned area.

c. Completion of training related to AIS security.

d. Experience in operation and use of AIS hardware and software within assigned area.

e. Geographically located in proximity of assigned workstations for effective surveillance.

f. Authorized user for all systems accessed from assigned workstations.

g. Possession of a security clearance for highest level of classified information processed on assigned workstations.

# CHAPTER 3

## COMSC AUTOMATED INFORMATION SYSTEMS SECURITY ENVIRONMENT

**3.1 AIS SECURITY ENVIRONMENT.** COMSC AIS security environment encompasses all equipment described in scope of this plan in use at MSC Headquarters

**3.2 HARDWARE.** COMSC is developing AIS based on a two tier system consisting of mainframe host systems as upper tier and desktop microcomputers as the lower tier. Currently COMSC hardware is a mix of workstation[1]/ types. MSC obtains mainframe support from Naval Computer and Telecommunications Station (NCTS), Washington DC. A detailed list of computer hardware that comprises MSC Headquarters AIS installations is on file in the master hardware inventory maintained by the Communication and Network Management Division (N62) of the Command, Control, Communication and Computer Systems (C4 Systems) Directorate (N6).

**3.3 SOFTWARE.** MSC is developing mainframe host systems under MVS/XA operating system using IDMS/R and BASIS for databases, and various programming languages for system development. Micro-computer software includes Infogate, Enable, DBase and other packages under MS/DOS operating system. A small number of Apple MacIntosh microcomputers utilize software specifically designed for such systems. MSC microcomputers and other workstations also make use of a variety of other software products to accomplish special tasks. N62 maintains the master software inventory for workstations. NCTS maintains an inventory of the software available on the mainframe host systems.

NOTE: The inventories maintained by N62, as specified in paragraphs 3.2 and 3.3 are considered as part of this AISSP for purpose of satisfying paragraph H.2.1, item a(10) of Appendix H to OPNAVINST 5239.1A.

**3.4 PHYSICAL FACILITY/SECURITY.** MSC Headquarters is located at Washington Navy Yard, Washington DC. The buildings occupied by MSC have restricted access and contain several Controlled Spaces (CSs) within which more sensitive work takes place.

---

[1]/ A workstation is defined as any electronic device capable of storing in memory, or on any media, any form of data, instructions or programs. and any electronic device used to communicate with a host computer or any size. This includes. but is not limited to, microcomputers, intelligent and dumb terminals, memory typewriters, word processors and Office Information Systems (OIS). The single exception is programmable, hand-held calculators for which no means exists with which data or programs can be exchanged with other than

another hand-held calculator.

**3.5 PERSONNEL.** MSC personnel are cleared as required for work they perform. Access to AIS resources includes requirement for proper security clearances and a need to know. Personnel working within a CS are cleared at the appropriate level, and visitors to these spaces are under escort or continuous surveillance.

**3.6 COMMUNICATIONS.** Currently communications within MSC are effected through the use of a mixture of commercial telephone lines, commercial dedicated lines, Defense Data Network (DDN), a node of WWMCCS, Tymnet and Telenet. All communication of classified material involving use of AIS resources is accomplished through use of encryption.

**3.7 EMANATIONS.** MSC adheres to OPNAVINST C5510.93E for control of compromising emanations. MSC has appointed a TEMPEST Control Officer (TCO) as required by OPNAVINST C5510.93E. ADPSO works with TCO as required to ensure compliance by AIS resources.

**3.8 ADMINISTRATIVE/OPERATING PROCEDURES.** MSC policy regarding the planning, design, development, implementation, operation, maintenance and approval of AIS is defined in COMSCINST 5223.1B, Information Resource Management Program, of 30 September 1986.

**3.9 DATA.** MSC processes classified, sensitive unclassified, and unclassified data with highest classification level being SECRET. The percentage of classified data processed is below 10% of total MSC workload, with unclassified data being majority of workload.

# CHAPTER 4

## AUTOMATED INFORMATION SYSTEMS SECURITY TRAINING

**4.1 INTRODUCTION.** Greatest threat to security and capability of MSC AIS installations is the inadvertent action of a user improperly handling classified media, deleting files or otherwise handling equipment and software in an improper manner or with disregard for security procedures. Similarly, a well informed user is best first line defense in any AIS security program. To this end, MSC personnel will be provided with training opportunities that include AIS security as well as the use of hardware and software.

**4.2 TRAINING POLICY.** Training in the use of each system developed or acquired for use by MSC is responsibility of the Functional Sponsor (FS) and Program Manager (PM) for the particular system in question. Such training will include any unique security requirements generated by specific system. The ADPSSO will assist FS and PM in training effort to ensure adequate coverage of security issues.

**4.2.1** Periodic security awareness training is responsibility of ADPSO, with assistance from AISPOs and TASOs. This training is required by Public Law 100-235, Computer Security Act of 1987, 8 January 1988. Annual reviews of AIS security as applicable to various systems and projects is responsibility of AISPSOs with assistance from applicable TASOs.

**4.2.2** Personnel who are new to MSC, as well as those who are new to using computers within MSC, are to enroll in an approved security course such as offered by NCTS. An acceptable alternative is to attend an MSC training session on AIS security, or to receive individual instruction from a member of MSC AIS Security Staff. Use of alternative methods must be documented with the ADPSO.

**4.3 AIS SECURITY CURRICULUM.** AIS Security Staff is responsible for developing and providing general AIS Security Training. Project Manager and Functional Sponsor are responsible for developing and providing AIS Security Training as it applies to their specific areas of responsibility. In both cases, such training will address requirements of this AISSP and below listed directives. Amount and depth of training in each subject area is dependent on who is being trained. Individual training plans may include in-house training and training offered by other activities.

a. Public Law 100-235, Computer Security Act of 1987

b. DOD Directive 5200.28 of 21 March 1988

c. OPNAVINST 5239.1A, Chapter 10 and Appendix D

**4.4 AIS SECURITY STAFF.** Security staff, with the exception of TASOs, will be knowledgeable in subject areas listed below. TASOs will be knowledgeable of items a, b, g, j, k and m, as required to comply with requirements of paragraph 2.3.4.

a. General Security Awareness. An overview of the scope of computer abuse, DON AIS Security Program, laws, regulations, and procedures for establishing and executing MSC AIS security program.

b. User and Customer Security. Users risk associated with receiving AIS services and in determining responsibility and protection requirements for user data security and integrity.

c. Security Administration. All parts of AIS security program administration, implementation, risk management and contingency planning and their interrelationships.

d. Change Control and Security Violation Reporting. Procedures for managing any change to AIS configuration and reporting security violations to appropriate DON officials.

e. Software Security. This area includes all types of application, operating systems and software controls and countermeasures that can reduce threats associated with processing different levels of data.

f. Telecommunication Security. Identification of all telecommunications safeguards that are available to reduce threats associated with transmitting different levels of data.

g. Terminal and Device Related Security. Controls and countermeasures that must be adhered to by users and customer to protect data.

h. Systems Design Security. Controls and countermeasures that must be built into design of an AIS application to meet level of security required by user and customer.

i Hardware Security. Identification of controls and countermeasures that are available to reduce threats associated with processing different levels of data. In addition, differences between hardware and software countermeasures must be evaluated and discussed.

j. Physical Security. Security requirements and countermeasures for physical protection of all AIS resources.

k. Personnel Security. Personnel security requirements associated with human resources when performing AIS operations.

l. Computer Auditing. Auditing principles, methods, tools, techniques and responsibilities required for periodic examination and evaluation of computer system procedures, controls and data.

m. Data Security. Identification of levels and types of data and the appropriate countermeasures to protect data.

n. Risk Assessment Methodology. Steps associated with conducting an activity Risk Assessment, computing the Annual Loss Expectancy and selecting cost-effective countermeasures to protect AIS assets.

o. Contingency and Backup Planning. Identification and documentation of a systematic method of response to any type of AIS operation disruption or emergency situation.

p. AIS Security and Navy Contractors. Interface between Industrial Security Regulations, Industrial Security Manual, Navy Security Regulations, Defense Intelligence Agency Regulations, Defense Communication Agency Regulations and those from National Security Agency, which must be reconciled during AIS system accreditation process.

q. Disaster Recovery. Requirements and procedures to develop an activity disaster recovery plan for AIS resources.

r. Security Accreditation. Security review and approval requirements for all DON AIS systems, and steps that must be taken to have AIS systems accredited.

s. Security Test and Evaluation. Identification and documentation of a systematic method for testing all security countermeasures associated with AIS systems and determining if all required countermeasures are being utilized.

# CHAPTER 5

## AUDIT AND INTERNAL REVIEW

**5.1 INTERNAL REVIEW SCHEDULE AND TEAM MEMBERSHIP.** MSC will conduct an internal review, including AIS security programs, at least every 3 years. Reviews will be conducted more frequently if there are significant changes or addition to systems which alter system's security posture or if there is a security violation or other situation that appears to invalidate original conditions of an accreditation. Members of review team will be determined by COMSC with assistance from N6 and the ADPSO.

**5.2 COMPLIANCE RESPONSIBILITY.** First line responsibility for ensuring compliance with AIS security directives lies with COMSC, Directors, AIS security staff, AIS Project Manager and individual user(s).

**5.3 COMPONENTS OF THE SECURITY REVIEW.** Investigators will review the following areas:

a. Accreditation Documentation

b. Risk Assessment

c. Contingency Plans or Memoranda

d. Security Test and Evaluations (ST&E)

e. Incident Reports

f. General Areas of Review

(1) Fraud, waste and abuse

(2) Accidental or deliberate disclosure of information to unauthorized persons

(3) Risk of financial loss

(4) Infringement on personal privacy or acts contrary to the Privacy Act of 1974

(5) Unauthorized destruction or modification of data

(6) Unauthorized use of DON (IS) resources

**5.4 SECURITY INCIDENT REPORTS.** Security incidents involving AIS will be investigated to determine their cause and appropriate corrective action needed. All incidents will be fully documented and handled in accordance with the provisions of OPNAVINST 5239.1A. The assistance of the Security Officer (N15) will be obtained in processing security incident reports.

**5.5 FRAUD, WASTE AND ABUSE ACITONS.** COMSC and Inspector General (IG) will be notified immediately if abuse, fraud or deliberate criminal actions are discovered. Investigative and prosecutable jurisdiction under the UCMJ and other penal and civil statutes will be coordinated under provisions of SECNAVINST 5520.3 (NOTAL).

# CHAPTER 6

## LIFE CYCLE MANAGEMENT (LCM)

**6.1 LCM SECURITY REQUIREMENTS.** Major LCM security requirements are addressed in a Security Annex of each MSC System Decision Paper (SDP) beginning at concept development phase. MSC system development policy requires that adequate security procedures be designed and maintained throughout entire life cycle of each MSC system and subsystem. Appendix I of OPNAVINST 5239.1A outlines security and audit controls to be addressed during life cycle.

**6.2 AIS PROJECT MANAGER LCM RESPONSIBILITIES.** As indicated in paragraph 2.2.4(b), it is the responsibility of each AIS Project Manager to ensure that all AIS security requirements are addressed throughout entire life cycle of a project. Security is to be addressed starting at concept development phase. AIS Project Manager is responsible for coordinating with rest of the AIS security staff to ensure that each system is in full compliance with all applicable security policies, procedures and regulations. This includes the development of a requirement for testing AIS security features.

**6.3 CLASSIFIED AND SENSITIVE DATA.** Systems processing Classified and Unclassified Sensitive information are to be identified at earliest possible LCM phase. Each project will include a statement in Security Annex of the SDP indicating the appropriate relative proportion of classified, sensitive unclassified and unclassified data.

**6.4. RISK INDEX.** Risk Index is to be computed for any AIS processing classified information as soon as possible in the life cycle. If the Risk Index is not 0 (zero), then it is possible that COMSC will not be authorized as DAA. This Risk Index can be used to determine the minimum security evaluation class for computer-based controls. Methodology provided in enclosure (4) of DOD Directive 5200.28 is to be used. Once this is determined, Figures 3-1 through 3-3 of OPNAVINST 5239.1A can be used to determine DAA. COMSC approval is required for continued funding, development and operation of any AIS requiring a DAA other than COMSC.

# CHAPTER 7

# CONFIGURATION MANAGEMENT

**7.1 CONFIGURATION MANAGEMENT.** All changes to hardware and software configurations will be requested via AIS Project Manager (PM) and Functional Sponsor (FS). The requests are reviewed and approved by Command, Control, Communication and Computer (C4) Systems Director (N6), the Information System Review Board (ISRB) and DAA. PMs and FSs are also responsible for notifying the ADPSSO and the ADPSO of the approved changes in configuration. ADPSSOs are responsible for evaluating impact of changes on security posture of AIS. The ADPSO will evaluate impact of changes on entire MSC AIS. ADPSSO and ADPSO will provide PM and FS with guidance in obtaining reaccreditation.

**7.1.1** At no time will users modify software applications, without first obtaining approval from the PM and FS. Unauthorized changes immediately invalidate previous accreditation and require a reaccreditation by DAA.

# CHAPTER 8

# CONTINGENCY PLANNING

**8.1 CONTINGENCY PLANS.** Due to importance of the services provided by AIS it is imperative that every reasonable effort be expended to assure their continuous operation. Contingency plans are designed to prepare users of AIS to continue their mission during abnormal operating conditions. A contingency plan is required for any AIS system or network for which unplanned disruption of service would have a critical impact on mission accomplishment. If unplanned disruptions of services would not have a critical impact on mission accomplishments, then DAA can dispense with a contingency plan.

**8.2 MANDATORY PROCEDURES.** The Functional Sponsor (FS) is responsible for determining whether or not a contingency plan is required. If the FS determines that a contingency plan is not required, then a memorandum will be prepared to the DAA by the FS requesting that requirement for a contingency plan be deleted. A copy of this memorandum will be forwarded to the ADPSO. DAA will make final determination as to requirement for a contingency plan with notification to the FS and ADPSO. The Project Manager (PM) is responsible for the preparation, documentation, testing and evaluation of the contingency plan. In addition, PM is responsible for annual evaluations of the contingency plan as in specified in paragraphs 7.3 through 7.7, and Figure H-5 of OPNAVINST 5239.1A. Contingency plans will be developed by project personnel with guidance from ADPSO, in most cases the contingency plan will be assigned to ADPSSO.

**8.3 SCOPE OF THE CONTINGENCY PLAN.** The contingency plan should identify:

a. Actions required if normal AIS environment is impaired or disrupted.

b. Actions required if functional application or user is denied information or service.

c. Actions required if AIS activity suddenly had to expand processing capability to accommodate a national emergency or some other critical event.

**8.4 GENERAL GUIDANCE.** MSC utilizes NCTS host systems and various standard communication networks. The PM is to determine extent of existing contingency plans for such systems and ability of these plans to satisfy MSC requirements. In those cases where existing contingency plans are inadequate, best solution may be to task NCTS or another responsible command or agency to update their contingency plan. If an existing contingency plan is adequate to protect MSC's interests, then PM can request that DAA dispense with requirement for a MSC contingency plan. Procedure to be followed is identical to that specified for an FS in paragraph 8.2 of this chapter.

# CHAPTER 9

# ACCREDITATION AND CERTIFICATION

**9.1 ACCREDITATION REQUIREMENTS.** COMSC is DAA for all MSC AIS, and as such, is solely responsible for granting accreditation as specified in OPNAVINST 5239.1A. ADPSO will coordinate the submission of all requests for accreditation or reaccreditation to DAA. Accreditation or an interim authority to operate is required before any AIS is placed into operation. An accreditation is valid for a maximum of 3 years. Reaccreditation is required prior to lapse of an accreditation or upon any changes to a system. Accreditation requires completion of following:

a. Activity Accreditation Schedule (AAS) form as contained in Appendix I.

b. Compliance with this AISSP including requirements of Appendix H, and development of an addendum to this AISSP to cover specific requirements of each project or related group of projects.

c. Compliance with OPNAVINST 5239.1A.

d. Conduct a risk assessment, as specified in Appendix F.

e. Development of an ST&E Plan and conduct of an ST&E, as specified in Appendix G.

f. Documentation of the ST&E test results, as specified in Appendix G.

g. Development of a Contingency Plan as specified in Chapter 8.

h. Submission of Accreditation Support Documentation as specified in Appendix I.

i. Issuance of a Statement of Accreditation by DAA as specified in paragraph 3.3.c of OPNAVINST 5239.1A.

j. Forwarding of a copy of Statement of Accreditation to COMNAVDAC.

k. Providing logistic and administrative support to ST&E team if external from MSC Headquarters.

l. Funding of technical assistance if local assistance is requested from NAVCOMTELCOM.

m. Other items as requested by DAA, ADPSO or N6.

**9.2 MSC ACCREDITATION.** The ADPSO develops and maintains the Activity Accreditation Schedule (AAS) for MSC Headquarters as a whole. The MSC AAS is maintained under a separate cover so it can be more readily updated. The AAS is considered as part of this AISSP for purpose of satisfying paragraph H.2.1, item a(10) of Appendix H to OPNAVINST 5239.1A. This accreditation is limited to off shelf software and hardware installed at MSC Headquarters that is not part of a network or other system accredited by other than MSC's DAA and that is not part of a Project Accreditation as described in paragraph 9.3, below. MSC may have AISs in one or more of the following categories, however, as specified in paragraph 3.3 of OPNAVINST 5239.1A, this will not limit the ability to accredit MSC at an activity level. This AISSP allows for inclusion of accreditation support documentation for AISs in Appendix J.

a. AISs for which all cost effective countermeasures have been implemented. These AISs will have received Project Accreditation.

b. AISs with an acceptable level of risk but with some cost effective countermeasures not yet implemented. These AISs may operate under an interim authority to operate which specifies the date for termination of this status and any special conditions that must be met.

c. AISs with an unacceptable level of risk, which must cease operations until corrective measures have been implemented. These AISs are specific exceptions to the MSC statement of accreditation.

**9.3 PROJECT ACCREDITATION OR CERTIFICATION.** MSC AIS projects require either accreditation or certification[1]. Certification is required for projects that will be installed, and included within accreditation of, an activity under control of a DAA other than accreditation of, an activity under control of a DAA other than COMSC. Accreditation is required for all other projects. If Risk Index, as described in enclosure (4) of DOD Directive 5200.28, is other than 0, the DAA for accreditation may be other than COMSC.

**9.3.1** Project Accreditation Where COMSC Is DAA. Program Manager (PM), with assistance from the ADPSSO, is responsible for developing and maintaining AAS for the entire life cycle of a project. A copy of AAS and other supporting documentation is forwarded to ADPSO as part of request for accreditation. This accreditation applies to all

1 - **Certification** is technical process evaluation, made as part of and in support of the accreditation process, whereby a procedure, program, system component or system is shown to be secure; i.e., that security design specifications are correct and have been properly implemented.

modifications and enhancements to off the shelf software and hardware, to any special purpose off the shelf software and hardware, as well as to any system developed for use by or within MSC Headquarters. Off the shelf software and hardware that is enhanced, modified or used within a project is to be covered by project AAS unless exempted by APDSO or DAA.

**9.3.2** Project Accreditation Where COMSC Is Not DAA. Accreditation requirements will be set by applicable DAA. MSC AIS Security Staff is not involved in determining or enforcing these requirements unless agreed to by COMSC. These situations will only occur where Risk Index results in a minimum security evaluation class for computer-based controls that exceeds DAA authority for COMSC as set forth in OPNAVINST 5239.1A.

**9.3.3** Project Certification. PM, with assistance from ADPSSO, is responsible for obtaining certification of all projects that do not require accreditation by a DAA. The certification will be approved and documented in same manner as required for a Project Accreditation. Scope of requirements for certification is less than for accreditation in that certification need only address those parts of accreditation requirements that are within control of the project. For example, certification of a single program need not address physical security of the hardware, nor security provided by system in which program executes. Certification documentation must state any expectations of environment (hardware, software and network) required for certification is for software installed at other commands. In such cases, the DAA for that command may establish specific certification requirements to be used in lieu of the requirements of this AISSP.

**9.4 INTERIM AUTHORITY TO OPERATE.** DAA may grant an interim authority to operate in lieu of accreditation. This authority is based upon an approved AISSP, or addendum, and is contingent upon meeting those conditions recommended by ADPSO and approved by DAA. This interim authority to operate is granted for a maximum time period of one year, and is not a waiver of the requirement for accreditation. An interim authority to operate is requested in same manner as used to request accreditation.

# APPENDIX A

## PART I - DEFINITIONS

The following definitions were taken from OPNAVINST 5239.1A, and updated and expanded based on DOD Directive 5200.28.

**ACCEPTABLE LEVEL OF RISK.** A judicious and carefully considered assessment by appropriate Designated Approving Authority (DAA) that an automatic data processing (ADP) activity or network meets minimum requirements of applicable security directives and provisions of OPNAVINST 5239.1A. Assessment should take into account value of ADP assets; threats and vulnerabilities; countermeasures and their efficacy in compensating for vulnerabilities and operational requirements. (DON)

**ACCESS.** A specific type of interaction between a subject (i.e., person, process or input device) and an object (i.e., an AIS resource such as a record, file, program, output device) that results in the flow of information from one to another. Also ability and opportunity to obtain knowledge of classified, sensitive unclassified or unclassified information. (DOD Directive 5200.28 of 21 March 1988)

**ACCREDITATION.** A formal declaration by DAA that AIS is approved to operate in a particular security mode using a prescribed set of safeguards. Accreditation is official management authorization for operation of an AIS and is based on certification process as well as other management considerations. The accreditation statement affixes security responsibility with DAA and shows that due care has been taken for security. (DOD Directive 5200.28 of 21 March 1988)

**ADP RESOURCES.** All ADP equipment, personnel, software, supplies, facilities and data/information used to support an automated process or function. (DON)

**AIS SECURITY.** Measures and controls that safeguard or protect an AIS against unauthorized (accidental or intentional) disclosure, modification or destruction of AISs and data, and denial of service. AIS security includes consideration of all hardware and/or software functions, characteristics and/or features; operational procedures, accountability procedures and access controls at the central computer facility, remote computer and terminal facilities; management constraints; physical structures and devices and personnel and communication controls needed to provide an acceptable level of risk for the AIS and for data and information contained in the AIS. It includes the totality of security safeguards needed to provide an acceptable protection level for an AIS and for data handled by an AIS. (DOD Directive 5200.28 of 21 March 1988)

**ADP SYSTEM.** An assembly of computer equipment, facilities, personnel, software and procedures configured for the purpose of structuring, sorting, calculating, computing, summarizing, storing and retrieving data and information with a minimum of human intervention. An ADP system as defined for purposes of OPNAVINST 5239.1A is the totality of automatic data processing equipment (ADPE) and includes:

a. General and special purpose computers (e.g., digital, analog or hybrid computer equipment);

b. Commercially available components, those produced as a result of research and development and the equivalent systems created from them, regardless of size, capacity or price, which are utilized in creation, collection, storage, processing, communication, display or dissemination of data;

c. Auxiliary or accessory equipment, such as data communications terminals, source data automation recording equipment (e.g., optical character recognition equipment, paper tape typewriters, magnetic tape cartridge typewriters and other data acquisition devices), data output equipment (e.g., digital plotters and computer output microfilmers), etc., to be used in support of digital, analog or hybrid computer equipment, either cable-connected, wire-connected or self-standing;

d. Electrical accounting machines used in conjunction with or independently of digital, analog or hybrid computers and

e. Computer equipment which supports or is integral to a weapons system. (DOD Directive 5200.28 of 18 December 1972)

**ASSURANCE.** A measure of confidence that security features and architecture of an AIS accurately mediate and enforce the security policy. If security features of an AIS are relied on to protect classified or sensitive unclassified information and restrict user access, features must be tested to ensure that security policy is enforced and may not be circumvented during AIS operation. (DOD Directive 5200.28 of 21 March 1988)

**AUDIT.** An independent review and examination of system records and activities to test for adequacy of system controls, to ensure compliance with established policy and operational procedures and to recommend any indicated changes in controls, policy or procedures.

**AUDIT TRAIL.** A chronological record of system activities that is sufficient to enable reconstruction, reviewing and examination of the sequence of environments and activities surrounding or leading to an operation, a procedure or an event in a transaction from its inception to final results. (DOD Directive 5200.28 of 21 March 1988)

**AUTOMATED INFORMATION SYSTEM (AIS).** An assembly of computer hardware, software, and/or firmware configured to collect, create, communicate, compute, disseminate, process, store and/or control data or information. (DOD Directive 5200.28 of 21 March 1988)

**CATEGORY.** A grouping of classified or sensitive unclassified information to which an additional restrictive label is applied for signifying that personnel are granted access to information only if they have formal access approval or other applicable authorization (e.g., proprietary information, for official use only, compartmented information). (DOD Directive 5200.28 of 21 March 1988)

**CENTRAL COMPUTER FACILITY.** One or more computers with their peripheral and storage units, central processing units and communications equipment in a single controlled area. This does not include remote computer facilities, peripheral devices or terminals which are located outside the single controlled area even though they are connected to the central computer facility by approved communication links. (DOD 5200.28-M of January 1973)

**CERTIFICATION.** Technical evaluation of an AISs security features and other safeguards, made in support of accreditation process, which establishes the extent that a particular AIS design and implementation meet a set of specified security requirements. (DOD Directive 5200.28 of 21 March 1988)

**COMPROMISING EMANATIONS.** Unintentional data relayed or intelligence-bearing signals which, if intercepted and analyzed, disclose the classified information transmission received, handled or otherwise processed by any information processing equipment. TEMPEST is an unclassified short name referring to investigations and studies of compromising emanations. It is sometimes used synonymously for "compromising emanations." (DON)

**COMPUTER.** A machine capable of accepting, performing calculations on or otherwise manipulating or storing data. It usually consists of arithmetic and logical units and a control unit and may have input and output devices and storage devices. (DOD Directive 5200.28 of 21 March 1988)

**CONFIGURATION MANAGEMENT.** Use of procedures appropriate for controlling changes to a system's hardware and software structure for the purpose of insuring that such changes will not lead to decreased data security. (DON)

**CONTINGENCY PLANS.** A plan for emergency response, backup operations and post-disaster recovery maintained by an ADP activity as a part of its security program. A comprehensive consistent statement of all actions (plan) to be taken before, during and after a disaster (emergency condition), along with documented, tested procedures which, if followed, will ensure availability of critical ADP resources and which will facilitate maintaining the continuity of operations in an emergency situation. (DON)

**CONTROLLED AREA.** An area within which uncontrolled movement does not permit access to classified information and which is designed for principal purpose of providing administrative control, safety or a buffer area of security restrictions for Limited Exclusions Areas. This are may be protected by physical security measures, such as sentries and fences. (Military Handbook 232)

**COUNTERMEASURE.** Any action, device, procedure, technique or other measure that reduces vulnerability of an ADP system or activity to realization of a threat. (DON)

**DATA.** A representation of facts, concepts, information or instructions suitable for communication, interpretation or processing by humans or by an AIS. (DOD Directive 5200.28 of 21 March 1988)

**DATA INTEGRITY.** State that exists when data is unchanged from its source and accidentally or maliciously has not been modified, altered or destroyed. (DOD Directive 5200.28 of 21 March 1988)

**DATA LEVEL.** (DON)

a. Level I. Classified data. Usage of “Level I” term discontinued.

b. Level II. Unclassified data requiring special protection; e.g., Privacy Act, For Official Use Only, technical documents restricted to limited distribution. Usage of “Level II” term discontinued.

c. Level III. All other unclassified data. Usage of “Level III” term discontinued.

**DATA OWNER.** Authority, individual or organization who has original responsibility for data by statute, Executive order or Directive. (DOD Directive 5200.28 of 21 March 1988)

**DENIAL OF SERVICE.** Action or actions that result in inability of an AIS or any essential part to perform its designated mission, either by loss or degradation of operational capability. (DOD Directive 5200.28 of 21 March 1988)

**DESIGNATED APPROVING AUTHORITY (DAA).** Official who has authority to decide on accepting security safeguards prescribed for an AIS or official who may be responsible for issuing an accreditation statement that records decision to accept those safeguards. DAA must be at an organizational level, have authority to evaluate the overall mission requirements of AIS and to provide definitive directions to AIS developers or owners relative to the risk in security posture of the AIS. (DOD Directive 5200.28 of 21 March 1988)

**EMBEDDED SYSTEM.** An embedded system is one that performs or controls a function, either in whole or in part, as an integral element of a larger system or subsystem (e.g., ground support equipment, flight simulators, engine test stands or fire control systems). (DOD Directive 5200.28 of 21 March 1988)

**EVALUATED PRODUCTS LIST (EPL).** A documented inventory of equipment, hardware, software and /or firmware that have been evaluated against evaluation criteria found in DOD 5200.28-STD, "Department of Defense Trusted Computer System Evaluation Criteria," December 1985. (DOD Directive 5200.28 of 21 March 1988)

**FORMAL ACCESS APPROVAL.** Documented approval by a data owner to allow access to a particular category of information. (DOD Directive 5200.28 of 21 March 1988)

**HANDLED BY.** Term "handled by" denotes activities performed on data in an AIS, such as collecting, processing, transferring, storing, retrieving, sorting, transmitting, disseminating and controlling. (DOD Directive 5200.28 of 21 March 1988)

**INFORMATION.** Knowledge such as facts, data, or opinions, including numerical, graphic or narrative forms, whether oral or maintained in any medium. (DOD Directive of 21 March 1988)

**INFORMATION SYSTEM.** Organized collection, processing, transmission and dissemination of information in accordance with defined procedures, whether automated or manual. (DOD Directive 5200.28 of 21 March 1988)

**MODES OF OPERATION.** Security environment and method of operating an ADP system or network. Following modes of operation are applicable to OPNAVINST 5239.1A:

a. Compartmented Mode. Utilization of a resource-sharing computer system for concurrent processing and/or storage of: (1) two or more types of sensitive compartmented information (SCI), or (2) any type of SCI with other than SCI. For DON purposes, compartmented mode should not be considered equivalent to multilevel mode. (DON)

b. Controlled Security Mode

(1) An ADP system is operating in controlled security mode when at least some personnel (users) with access to system have neither a security clearance nor a need-to-know for all classified material then contained in the ADP system. However, the basis, respectively or security clearance and security classification is not essentially under operating system control as in multilevel security mode.

(2) This mode presents an alternative to encourage ingenuity in meeting security requirements of OPNAVINST 5239.1A in a manner less restrictive than the dedicated and system high security mode, but as a level of risk lower than that generally associated with true multilevel security mode. This is accomplished by implementation of explicit augmenting measures that reduce or remove a substantial measure of system software vulnerabilities together with specific limitation of personnel security clearance levels of users permitted concurrent access to the system.

(a) Examples of measures that augment or enhance system by reducing or removing system software vulnerabilities and associated risk include employment of hardware and/or firmware that is alterable only at the Central Computer Facility, for critical system security functions; employment of hardware/operating systems or systems architectures that manifest reduced system software vulnerabilities and risk; interconnection of remote terminals via one-way hardware and/or firmware information communications wherein substantive information can only be transmitted in one direction (some circuits require two-way communication for certain control information in order to receive substantive information properly-these may be considered one-way circuits when it is determined that only control information can be transmitted in two directions); assignment of terminal security officers in remote terminal areas not protected as required for highest classification category, most restrictive types(s) of material then being handled by system wherein the terminal security officer has a security clearance for that highest level; system splitting via hardware and/or firmware alterable only at the Central Computer Facility and/or limitation on user capabilities, such as restriction to fixed query access only or the prohibition of user assembled and machine language programming.

(b) Consideration shall also be given to specific limitation of number of separate personnel security clearance levels of users permitted concurrent access to the system to no more than three adjacent levels, including uncleared. For example, permitting access by uncleared users as well as users with Confidential and Secret security clearances and formal access authorizations for additionally restrictive types of classified material. Certain such additionally restrictive types of classified material may replace other limitations or requirements on the foregoing. (DOD 5200.28-M of January 1973)

c. Dedicated Security Mode. A mode of operation wherein all users have clearance or authorization and need-to-know for all data handled by AIS. If AIS processes special access information, all users require formal access approval. In dedicated mode, an AIS may handle a single classification level and/or category of information or a range of classification levels and/or categories. (DOD Directive 5200.28 of 21 March 1988)

d. Multilevel Security Mode. A mode of operation that allows two or more classification levels of information to be processed simultaneously within same system when not all users have a clearance or formal access approval for all data handled by AIS.

e. System High Security Mode. A mode of operation wherein all users having access to AIS possess a security clearance or authorization, but not necessarily a need-to-know, for all data handled by the AIS. If AIS processes special access information, all users must have formal access approval. (DOD Directive 5200.28 of 21 March 1988)

f. Limited ADP Access Security Mode. An ADP system or network is operating in limited access security mode when type of data being processed is categorized as unclassified and requires implementation of special access controls to restrict access to data only to individuals who by their job function have a need to access data. (DON)

g. Partitioned Security Mode. A mode of operation wherein all personnel have clearance, but not necessarily formal access approval and need-to-know, for all information handled by AIS. This security mode encompasses compartmented mode defined in Director of Central Intelligence Directive Number 1/16, "Security Policy on Intelligence Information in Automated Systems and Networks (U), "4 January 1983.

**NEED-TO-KNOW.** A determination made in interest of U.S. national security by custodian of classified or sensitive unclassified information which a prospective recipient for access to, knowledge of or possession of information to perform official tasks or services. (DOD Directive 5200.28 of 21 March 1988)

**NETWORK.** A network is composed of a communications medium and all components attached to that medium whose responsibility is transference of information. Such components may include AISs, packet switches, telecommunications controllers, key distribution centers and technical control devices. (DOD Directive 5200.28 of 21 March 1988)

**ORANGE BOOK TERMINOLOGY.** DOD Directive 5200.28-STD, "Department of Defense Trusted Computer System Evaluation Criteria," December 1985, also called Orange Book, classifies AISs into four broad hierarchical divisions of security protection. Within divisions C and B there are further subdivisions called classes. These classes also are ordered in a hierarchical manner characterized by the set of computer security features they possess (see Security Features, below). (DOD Directive 5200.28 of 21 March 1988)

**PERIODS PROCESSING.** A manner of operating an AIS in which security mode of operation and/or maximum classification of data handled by AIS is established for an interval of time (or period) and then changed for following interval of time. A period extends from any secure initialization of the AIS to completion of any purging sensitive data handled by AIS during period. (DOD Directive 5200.28 of 21 March 1988)

**PERSONAL DATA.** Data about an individual including, but not limited to, education, financial transactions, medical history, qualifications, service data, criminal or employment history which ties data to individual's name or an identifying number, symbol or other identifying particular assigned to individual, such as a finger or voice print or a photograph. (DON)

**PURGE.** Removal of sensitive data from an AIS at end of a period of processing, including from AIS storage devices and other peripheral devices with storage capacity, in such a way that there is assurance proportional to sensitivity of the data that data may not be reconstructed. An AIS must be disconnected from any external network before a purge. (DOD Directive 5200.28 of 21 March 1988)

**RISK.** A combination of likelihood that a threat shall occur, likelihood that a threat occurrence shall result in an adverse impact, and severity of resulting adverse impact. (DOD Directive 5200.28 of 21 March 1988)

**RISK ANALYSIS.** An analysis of system assets and vulnerabilities to establish an expected loss from certain events based on estimated probabilities of occurrence. (DOD Directive 5200.28 of 21 March 1988)

**RISK INDEX.** Disparity between minimum clearance or authorization of AIS users and the maximum sensitivity (e.g., classification and categories) of data handled by AIS. (DOD Directive 5200.28 of 21 March 1988)

**RISK ASSESSMENT.** An analysis of system assets and vulnerabilities to establish an expected loss from certain events based on estimated probabilities of occurrence of those events. Purpose of a risk assessment is to determine if countermeasures are adequate to reduce probability of loss or impact of loss to an acceptable level. (DON)

**RISK MANAGEMENT.** Total process of identifying, measuring and minimizing uncertain events affecting AIS resources. It includes risk analysis, cost benefit analysis, safeguard selection, security test and evaluation, safeguard implementation and systems review. (DOD Directive 5200.28 of 21 March 1988)

**SECURITY FEATURES.** Security-relevant functions, mechanisms and characteristics of AIS hardware and software (e.g., identification, authentication, audit trail, access control). (DOD Directive 5200.28 of 21 March 1988)

**SECURITY MODE.** A mode of operation in which DAA accredits an AIS to operate. Inherent with each of four security modes (dedicated, system high, multilevel and partitioned) are restrictions on user clearance levels, formal access requirements, need-to-know requirements and range of sensitive information permitted on the AIS. (DOD Directive 5200.28 of 21 March 1988)

**SECURITY SAFEGUARDS.** Protective measures and controls that are prescribed to meet security requirements specified for an AIS. These safeguards may include, but are not necessarily limited to, hardware and software security features; operation procedures; accountability procedures; access and distribution controls; management constraints; personnel security; and physical structures, areas and devices. (DOD Directive 5200.28 of 21 March 1988)

**SECURITY TEST & EVALUATION (ST&E).** An examination and analysis of security features of an ADP activity or network as they have been applied in an operational environment to determine the security posture of activity or network upon which an accreditation can be based. (DON)

**SENSITIVE BUSINESS DATA.** Data which requires protection under Title 18, USC 1905, and other date which by its nature requires controlled distribution or access for reasons other than fact that it is classified or personal data. Sensitive business data is recognized in following categories:

a. For Official Use Only -- Requiring confidentiality of information derived from Inspector General, authority or other investigative activity.

b. Financial -- Requiring protection to ensure integrity of funds or other fiscal assets.

c. Sensitive Management -- Requiring protection to defend against loss of property, material or supplies or to defend against disruption of operations or normal management practices, etc.

d. Proprietary -- Requiring protection to protect data or information in conformance with a limited rights agreement or which is exclusive property of a civilian corporation or individual and which is on loan to Government for evaluation or for its proper use in adjudicating contracts.

e. Privileged -- Requiring protection for conformance with business standards or as required by law. (Example: Government developed information involving the award of a contract.) (DON)

**SENSITIVE COMPARTMENTED INFORMATION (SCI).** Classified information about or derived from intelligence sources, methods or analytical processes that is required to be handled exclusively within formal access control systems established by Director, Central Intelligence. (DOD Directive 5200.28 of 21 March 1988)

**SENSITIVE UNCLASSIFIED INFORMATION.** Any information loss, misuse or unauthorized access to or modification of which adversely might affect U.S. national interest, the conduct of DOD programs or the privacy of DOD personnel (e.g., FOIA exempt information and information whose distribution is limited by DOD Directive 5230.24). (DOD Directive 5200.28 of 21 March 1988)

**SIOP-ESI.** An acronym for Single Integrated Operational Plan-Extremely Sensitive Information, a DOD Special Access Program. (DOD Directive 5200.28 of 21 March 1988)

**SPECIAL ACCESS PROGRAM.** Any program imposing need-to-know or access controls beyond those normally required for access to Confidential, Secret or Top Secret information. Such a program includes, but is not limited to, special clearance of investigative requirements, special designation of officials authorized to determine need-to-know or special lists of persons determined to have a need-to-know. (DOD Directive 5200.28 of 21 March 1988)

**TELECOMMUNICATIONS.** Under DOD Directive 5200.28 of 21 March 1988, a general term expressing data transmission between computing systems and remotely located devices via a unit that performs necessary format conversion and controls the rate of transmission.

**THREAT.** Any circumstances or event with potential to cause harm to ADP system or activity in form of destruction, disclosure and modification of data or denial or service. A threat is a potential for harm. Presence of a threat does not mean that it will necessarily cause actual harm. Threats exist because of very existence of system or activity and not because of any specific weakness. For example, the threat of fire exists at all facilities, regardless of the amount of fire protection available. (DON)

**TRUSTED PRODUCTS.** Products evaluated and approved for inclusion on Evaluated Products List (EPL). (DOD Directive 5200.28 of 21 March 1988)

**UNCLASSIFIED INFORMATION.** Any information that need not be safeguarded against disclosure, but must be safeguarded against tampering, destruction, or loss due to record value, utility, replacement cost or susceptibility to fraud, waste or abuse. (DOD Directive 5200.28 of 21 March 1988)

**USERS.** People or processes accessing an AIS either by direct connections (i.e., via terminals) or indirect connections (i.e., prepare input data or receive output that is not reviewed for content or classification by a responsible individual). (DOD Directive 5200.28 of 21 March 1988)

**VULNERABILITY.** A weakness in the physical layout, organization, procedures, personnel, management, administration, hardware or software that may be exploited to cause harm to the ADP system or activity. Presence of a vulnerability does not in itself cause harm; a vulnerability is merely a condition or set of conditions that may allow the ADP system or activity to be harmed by an attack. (DON)

# APPENDIX A

## PART II - ACRONYMS

| | |
|---|---|
| **AAS** | Activity Accreditation Schedule` |
| **ADP** | Automated Data Processing |
| **AIS** | Automated Information System |
| **ADPNSO** | Automated Data Processing Network Security Officer |
| **ADPSO** | Automated Data Processing Security Officer |
| **AISSP** | Automated Information Systems Security Plan |
| **ADPSSO** | Automated Data Processing System Security Officer |
| **CLIPS** | Classified Information Processing System |
| **COMSEC** | Communications Security |
| **COR** | Contracting Officer's Representative |
| **CS** | Controlled Space |
| **C4S** | Command, Control, Communication and Computer Systems |
| **DAA** | Designated Approval Authority |
| **DDN** | Defense Data Network |
| **DES** | Data Encryption Standard |
| **FIPS** | Federal Information Processing Standard |
| **FS** | Functional Sponsor |
| **ISRB** | Information Systems Resources Board |
| **ITS** | Instrumented TEMPEST Survey |
| **LAN** | Local Area Network |
| **LCM** | Life Cycle Management |
| **MSC** | Military Sealift Command |
| **NOTAL** | Not Transmitted to All |
| **N6** | Command, Control, Communication and Computer Systems Directorate |
| **N62** | Communication and Network Management Division |
| **N63** | Database and Data Administration Division |
| **OIS** | Office Information System(s) |
| **POA&M** | Plan of Action and Milestones |
| **SCI** | Special Compartmented Information |
| **SMIS** | Shipboard Management Information System |
| **ST&E** | System Test & Evaluation |
| **TASO** | Terminal Area Security Officer |
| **TCB** | Trusted Computer Base |
| **TCO** | TEMPEST Control Officer |
| **TVAR** | TEMPEST Vulnerability Assessment Request |
| **UIC** | Unit Identification Code |
| **WWMCCS** | World Wide Military Command and Control System |
| **WASSO** | WWMCCS ADP System Security Officer |

# APPENDIX B

# BIBLIOGRAPHY

Public Law 100-235 - Computer Security Act of 1987, 8 January 1988

DOD 5200.1-R - Information Security Program Regulation, June 1986

DOD Directive 5200.28 - Security Requirements for Automated Information Systems (AISs), 21 March 1988

DOD 5200.28-STD - DOD Trusted Computer System Evaluation Criteria, December 1985

SECNAVINST 5231.1C - Life Cycle Management Policy and Approval Requirements for Information System Projects, 10 July 1992

SECNAVINST 5239.2 - DON Automated Information Systems (AIS) Security Program, 15 November 1989

OPNAVINST 5239.1A - DON Automatic Data Processing Security Program, 3 August 1982

OPNAVINST 5510.1H - DON Information and Personnel Security Program Regulation, 29 April 1988

OPNAVINST C5510.93E - Navy Implementation of National Policy on Control of Compromising Emanations (U), 22 February 1988

COMSCINST 5223.1B - Information Resource Management Program, 30 September 1986

CSC-STD-003-85 - Computer Security Requirements--Guidance for Applying the DOD Trusted Computer System Evaluation Criteria in Specific Environments, 25 June 1985

CSC-STD-005-85 - DOD Magnetic Remanence Security Guideline, 15 November 1985

CSC-STD-002-85 - DOD Password Management Guideline, 12 April 1985

NCSC-TG-005 Version 1 - Trusted Network Interpretation of The Trusted Computer System Evaluation Criteria, 31 July 1987

# APPENDIX C

## DOD AND DON AIS SECURITY POLICIES

Contents of this appendix were taken directly from OPNAVINST 5239.1A. However, this appendix is not a complete copy of all DON policies as stated in that instruction.

**C.1 DOD AIS SECURITY POLICIES.** DOD AIS security policies are:

a. Individual accountability. AIS system users will be identified by appropriate administrative or hardware and software measures. Access to an activity within AIS system will be controlled and monitored.

b. Physical control. AIS activity or network will be externally protected against unauthorized access to entry points, access to data or damage to the activity. Area that is externally protected is designated the controlled area.

NOTE: The above designation of a controlled area should not be confused with a Controlled Space as used in OPNAVINST C5510.93E when discussing CLIPS.

c. System stability. All elements of AIS system or network will function in a cohesive, identifiable, predictable and reliable manner so that malfunctions are detected and reported within a known time.

d. Data integrity. Each file or collection of data in AIS system or network will have an identifiable origin and use. Its use, backup, accessibility, maintenance, movement and disposition will be governed on basis of level and type of data, need to know and other sensitive measures, as appropriate.

e. Access limits. AIS system or network will function so that each user has access to all of data to which user is entitled, but no more.

f. Communication links. AIS system communication links and lines will be secured in a manner appropriate for the level of data they transmit.

g. Levels I, II and III material, (usage of these terms is discontinued; will use instead: classified, sensitive unclassified, unclassified). Material handled and produced by an AIS activity, such as storage media or output materials, will be safeguarded as appropriate for level of data assigned and will bear appropriate security markings in eye-readable form.

**C.2 DON AIS SECURITY POLICIES.** DON AIS security policies are:

a. Mandatory procedures for risk assessment, ST&E and contingency planning described in OPNAVINST 5239.1A are required.

b. A risk assessment will be conducted when developing a new AIS system or network and for each AIS activity or network. Risk assessments will be conducted at least every 3 years or whenever, in judgment of the commander, a system configuration or facility change has been effected that impacts security policy of AIS activity or network.

c. The commander will not obtain contractor assistance in conducting a risk assessment, an ST&E or a contingency test before formally requesting technical assistance from the Commander, Naval Data Automation Command (COMNAVDAC).

d. When a peripheral or remote device is to be connected to an AIS system or network processing classified or sensitive unclassified data and will be used by personnel of an activity that is not responsible for security of host AIS system or network, security measures for the peripheral or remote device and its controlled area will be prescribed by activity responsible for the security of host AIS system or network. This applies whether or not peripheral or remote device is approved for handling classified, sensitive unclassified or unclassified data. Such security measures will be agreed to, formally documented and implemented before peripheral or remote device is connected to host AIS system or network.

e. OPNAVINST C5510.93E (NOTAL) contains requirements and responsibilities for compliance with DON and national policy on TEMPEST. In procurement of new AIS hardware planned for processing classified data, consideration will be given to obtaining operationally suitable equipment designed to minimize compromising emanations.

f. AIS security documentation disclosing vulnerabilities or exploitation techniques in sufficient detail to enable convert penetration of an AIS activity or network processing classified or sensitive unclassified data will be marked at least “For Official Use Only.”

g. Software and files providing internal security controls, passwords or audit trails for AIS systems or networks will be safeguarded to prevent unauthorized modification.

h. Use of Data Encryption Standard (DES) is prohibited for AIS systems or networks processing classified data.

i. With advent of mini/microcomputers, microcode (firmware), fiber optics, satellite-assisted telecommunication interfaces and other technological improvements, many products available commercially are not sanctioned for use by DON AIS activities. Plans implementing these technologies for classified data processing should include ascertaining if these products are to be endorsed for DON use.

# APPENDIX D

## SECURITY OF AIS MEDIA

**D.1 INTRODUCTION.** Data and information, whether unclassified or classified, are represented and stored on many different substances and materials within the environment. These various forms are collectively referred to as AIS media. AIS media includes carbon paper, cathode ray tube (CRT) displays, computer output microfilm/ microfiche, disks, core storage units, diskettes, hard copy output, magnetic tape, mass memory storage units, optical disks, paper tape, printer ribbon, punch cards and other devices. This appendix provides details for media currently in use at MSC Headquarters. Requirements for other media, such as punched cards, are provided in OPNAVINSTs 5239.1A and 5510.1H. There are two categories of AIS media: working copy media and finished copy media.

a. Working copy media is temporary in nature (retained for 180 days or less) and stays within the confines and control of MSC. This type of media includes media which is used and updated at frequent intervals and media that is returned immediately to user after processing.

b. Finished media is permanent in nature and can be released outside of MSC only if released by other than electrical means. For example, magnetic tape can be shipped and will be receipted for as a finished media. When the tape is introduced into receiving activity, it may be treated as a working copy media if it satisfies conditions above. This type of media includes any media that is retained for more than 180 days.

**D.2 SECURITY CONTROLS.** These controls are the minimum essential controls for AIS media.

a. Working Copy Media

` (1) Unclassified working copy media may be maintained in any MSC Headquarters office without special protection. This media need not carry any labeling indicating that it is unclassified, although it is a good practice to label media to indicate contents and responsible individual. If media contains proprietary software or data it is not classified.

(2) Sensitive unclassified working copy media may be maintained in any MSC Headquarters office provided it is stored and handled so as to protect the media and its contents from compromise or other loss, damage, or unauthorized access. Media containing proprietary software or data is sensitive unclassified.

(3) Classified working copy media will be dated when created, marked with highest classification of any data contained on media, protected and destroyed when it has served its purpose. It will be stored in accordance with OPNAVINST 5510.1H. If classified working copy media are given to a user, user is responsible for their protection.

b. Finished Media

(1) Unclassified finished media will be controlled same as in subparagraph D2a(1).

(2) Sensitive unclassified finished media will be controlled same as in subparagraph D2a(2).

(3) Classified finished media will be marked, accounted for and controlled in same manner prescribed for classified material outside of an AIS environment. See OPNAVINST 5510.1H for appropriate guidance. Activity receiving classified finished media will provide user with a signed and dated receipt. An activity forwarding signed for upon release and will have a safeguard statement attached.

c. Printer Ribbons. Due to large variety of ribbons and printers in use, it is difficult to state with certainty that any and all classified information has been totally obscured from a given ribbon with a detailed examination of that ribbon. Therefore, printer ribbons should be controlled at highest level of information ever printed by that ribbon until that ribbon is destroyed. The same ribbon should be retained in printer for unclassified and classified information consistent with levels of physical security enforced for area. Procedures described in OPNAVINST 5510.1H for typewriter ribbons do not apply to printer ribbons and should not be used as a guide or authority for declassifying printer ribbons.

d. Destruction. AIS media, both classified and unclassified, will be destroyed as soon as it is not longer required. Unclassified AIS media will be disposed of in same manner as unclassified material outside of an AIS environment. Classified AIS media will be destroyed according to OPNAVINST 5510.1H. Prior to destroying magnetic media, media should be degaussed or otherwise prepared as required by OPNAVINST 5510.1H.

e. Inventories of Tapes, Disk Packs and Other AIS Media. MSC offices will maintain a master list of AIS media that is classified as SECRET or TOP SECRET and controlled as finished documents. This master list will include the overall security classification of media, special access category (if appropriate) and permanently assigned identification number.

## D.3 SECURITY MARKINGS

a. Removable storage media

(1) Removable information storage media and devices will be externally marked on a removable label with overall security classification, special category (if appropriate) and a permanently assigned identification number. These same devices will be marked internally with a recorded notation that indicates individual classification and special category (if appropriate). If tape, cassette or disk pack is classified, every set of records or file on the AIS media will identify the classification authority, date of creation, record owner, record classification and downgrading/declassification instructions.

(a) External labeling must be with color coded labels as follows:

1. SF 706 - Orange, Top Secret

2. SF 707 - Red, Secret

3. SF 708 - Blue, Confidential

4. FS 709 - Purple, Classified

5. SF 710 - Green, Unclassified

6. SF 711 - White, requires filling in classification

(b) Internal marking must be provided by all AIS, including word processing systems, to ensure that classified material which is reproduced or generated clearly shows classification and associated markings.

(2) When tapes, cassettes and disk packs are declassified by degaussing using an approved magnetic device or magnet, all external labels indicating the classification will be removed unless media will be immediately used to store information of same classification.

b. Hard Copy Reports. Hard copy reports or printouts from a line printer, terminal, plotter or other AIS equipment will be marked as follows:

(1) First page and front and back covers, if any, of documents produced by AIS will be marked as prescribed in OPNAVINST 5510.1H.

(2) Reports prepared during classified processing will be marked at top and bottom of each page with the appropriate classification or the word "UNCLASSIFIED."

(3) Page numbering and binding of classified reports are to be used when possible. Forewords, prefaces or special instructions may be bound as an AIS product, but will be in a separately numbered section or distinguished by Roman numeral page numbers to avoid renumbering of machine numbered pages.

(4) All classified material prepared by AIS will be marked in accordance with specific requirements of OPNAVINST 5510.1H as to format, placement and other details.

c. CRT Displays. All classified CRT displays will have appropriate security classification marking displayed at the top of screen. Hard copy reports generated from such a device will be marked as cited above.

**D.4 DECLASSIFYING AND CLEARING PROCEDURES.** Declassifying AIS media is a procedure to erase totally and unequivocally any and all classified information stored on that media. Clear AIS media is a procedure used to erase classified information, but totality and finality of declassifying are lacking. Distinction between the two procedures lies both in purpose for which each is done and specific manner and techniques employed. Clearing is used in a facility when media will remain within facility, and it is normally done because media are to be reused. Declassifying may be done for same reason (in the case of magnetic tapes and disk packs), but is required when media will be released outside facility, such as when equipment is turned in for repair outside the facility; for permanent turn-in; or for release to another facility, agency or activity. A record will be maintained for 2 years after AIS media is declassified.

a. Exceptions. Media containing certain types of information such as classified Communications Security keying material marked CRYPTOGRAPHIC will not be declassified or downgraded in accordance with the procedures described below. Such media will be safeguarded as required for highest classification of information ever recorded thereon until media are physically destroyed.

b. General. When media have been declassified as described below, all markings identifying previous source, use or classification will be removed. Media considered as working papers may be declassified or cleared without executing a certificate of destruction. Media controlled as finished documents may be deleted from master list by lining through the item, entering disposition, date of disposition and initials for individual deleting the item. No certificate of destruction is required for declassifying or clearing such magnetic media, if classification level is below SECRET.

c. Magnetic Tapes. Magnetic tapes may be declassified when degaussed by equipment and procedures. Magnetic tapes may be individually cleared by overwriting one time with any one character. However, cleared magnetic tapes will be safeguarded, controlled and marked at level commensurate with highest classification of information recorded on them before they were cleared.

d. Disks, Disk Packs, Drums, Screen and Other Rigid Magnetic Media. Such media may be declassified if completely overwritten at least three times, once with a binary digit "1," once with a binary digit "0" and once with any other alphanumeric or special character which will be left on the media. Last overwrite will be verified, such ad by attempting to read and print all characters other than character used for last overwrite. Electrical current used to accomplish overwrite will be at least equal to normal recording strength, and it will be sufficient to override any peaks or valleys which may have occurred in the power source during recording period. Inoperative equipment which cannot be overwritten may be declassified by exposing each recording surface to a magnet having a field strength of at least 1500 oersted. Entire recording surface (all tracks) will be wiped at least three times by a nonuniform motion of the magnet. A thin sheet of plastic (1-5 mil thick) should be used to prevent damage to the recording surfaces. Media of this type will be cleared by one level commensurate with highest classification of information recorded on them before clearing.

e. Internal Memory, Buffers, Registers and Similar Storage Areas. These storage areas will be declassified or cleared, as described below.

(1) These areas may be cleared by use of a hardware clear switch, a power-on reset cycle or a program designated to overwrite storage area. Periodic verification should be made that methods are working correctly. Verification may take form of random sampling or program read and compare.

(2) Volatile, read/write semiconductor memories may be declassified in whole or in part by setting a "zero" or "one" in all memory locations or by removal of power from system. This will be followed by a verification. This procedure is authorized provided the classified data has not resided undisturbed in memory for over 72 hours. This procedure does not apply to non-volatile semiconductor memories such as metal nitride oxide semiconductor memories or to read-only semiconductor memories.

(3) For declassifying ferromagnetic core memory refer to OPNAVINST 5239.1A.

(4) For declassifying all other media not specifically described in this AISSP, refer to OPNAVINST 5239.1A and OPNAVINST 5510.1H. In event that there is a conflict between these two instructions, matter will be determined by the AISSO.

f. CRT. Prior to the release or turn-in of a CRT which has been used to display classified information, each screen surface will be inspected under the highest intensity internal CRT illumination to detect evidence of burned-in information. If, after careful inspection, it is determined that no classified information has been etched into CRT phosphor, CRT may be considered declassified and released. CRT screens which contain burned-in classified information will either be retained within appropriate classified environment or be destroyed to preclude classified information from being recovered by unauthorized persons.

# APPENDIX E

## SECURITY GUIDANCE FOR WORSTATIONS

With widespread use of workstations[1], risk of loss, disclosure or compromise of classified and/or sensitive information processed on these units rises significantly. Because of accessibility of workstations and their inability to discriminate between "good" user and "bad" user, each MSC employee should observe the following practices to ensure a safe and secure computing environment.

**E.1** Workstation processing of both classified and unclassified (sensitive) data within MSC must be restricted to users with valid clearances for level of classification and a legitimate "Need to Know" data being handled. Processing is to be limited to minimum amount of data at lowest level of classification consistent with mission accomplishment.

**E.2** All offices using workstations to process classified data must provide same physical security as is afforded handling of classified hard copy documents.

**E.3** Limit access to your assigned workstation. Know identities of other personnel who may use your equipment, and check identity and credentials of persons who come to your office to repair it.

**E.4** Ensure that microcomputer equipment that processes classified information is not connected to non-secure telephone modems.

**E.5** Ensure that nonsecure telephones have a minimum separation of one meter from any AIS processing classified information. No AIS will be placed on the same metallic surface with a nonsecure telephone or intercom system.

**E.6** Note that Public Law 98-473 prohibits and establishes penalties for unauthorized access to, use or alteration of Government computer information.

---

1 - A **workstation** is defined as any electronic device capable of storing in memory, or on any media, any form of data, instructions or programs and any electronic device used to communicate with a host computer or any size. This includes, but is not limited to, microcomputers, intelligent and dumb terminals, memory typewriters, word processors and Office Information Systems (OIS). The single exception is programmable, hand-held calculators for which no means exists with which data or programs can be exchanged with other than another hand-held calculator.

**E.7** Magnetic media (diskettes, hard disks, tapes, etc.) must be labeled and handled at highest security level of the data stored on them. Safeguards for classified magnetic media are identical to those required for paper documents of same level as specified in COMSCINST 5510.8D.

a. Storage of classified data on magnetic media is limited to one security classification.

b. Classified magnetic media will be locked in a safe when not in use.

c. Delete/erase procedures should not be trusted to completely remove classified data from magnetic media. Contact the ADPSO for assistance in properly removing classified information from magnetic media.

d. Destruction, declassification and discarding magnetic media requires ADPSO approval. ADPSO involvement is required to ensure classified information will not be inadvertently compromised.

e. Classified data which is transferred to another media will retain the classification level originally assigned to data. Thus, receiving media must be labeled and handled at highest classification level of originating media.

f. Unclassified data which has been resident on classified media and is subsequently transferred to another media may carry with it some portion of classified data. As a result, receiving media must be labeled and handled at highest classification level or originating media.

**E.8** Beware of borrowed or unsolicited software. Such software may be designed to alter your data or application.

**E.9** Ensure that privately owned software is not used on government owned or government controlled AISs. Only software approved by authorized personnel and purchased by the government from legitimate commercial/government vendors/ developers will be loaded on government owned or government controlled AISs.

**E.10** Make back-up copies of your data files and applications and properly mark each one with same level of classification as original data. Backups of data should be made to physically separate media than that used to backup applications and other executable programs. Media used for backups should not be bootable, i.e., formatted with MS-DOS command “FORMAT d:/S.”

**E.11** Ensure that distribution diskettes for each operating system, commercial software and application software are stored in appropriate containers to ensure backup in the event of destruction of the working copy. Classified and unclassified data files will be independently backed up as necessary, to ensure minimum recovery time in the event of destruction.

**E.12** Note that data for MSC jobs, entered on microcomputer, regardless of ownership or location of the computer, is the property of MSC and may be official records. This includes job-related work voluntarily done at home on privately owned computers. Such data is subject to Federal statutes and regulations, such as the Federal Records Act, Privacy Act, Freedom of Information Act and MSC records disposition schedules.

**E.13** Ensure that privately owned microcomputers are not used in workspaces, unless a waiver is granted by commanding officer/DAA or ADPSO. Request for waiver will be submitted to DAA or ADPSO, signed by commanding officer/DAA or ADPSO and will include type of equipment, location, intended processing and clearing procedures for all hardware/software/data prior to removal and will include a statement of disclaimer for MSC liability for private property. All magnetic media used on privately owned AIS equipment will be labeled and accounted for in accordance with Appendix D and is the property of U.S. Navy.

**E.14** Ensure that MSC data created on a privately owned computer are readable in the absence of that computer.

**E.15** Ensure compatability of systems, data, storage media based on MSC needs, when privately owned microcomputers/hardware are brought into MSC offices.

**E.16** Protect passwords. Do not provide passwords, identification numbers or telephone access codes to unauthorized personnel. Keep your passwords to yourself. Do not tape any access codes to desks, microcomputers, printers, hard disks, wall space or other locations as they may become available to unauthorized personnel. Operate legitimately through password authorization process.

**E.17** Protect keyboard and screen from viewing while entering password.

**E.18** Properly safeguard, review and mark printed output.

**E.19** Label all diskettes. Indicate classification level of data or application on diskette. Unclassified or sensitive diskettes also should be labeled. Standard forms SF-706 through SF-711 are available for labeling magnetic media.

**E.20** Classified and sensitive data are not to be left in an unattended workstation.

**E.21** Logoff/Disconnect from any remote systems or network and turn workstation off at end of your shift or working day. This also applies to any extended periods of time, i.e., 30 minutes or more, during which workstation will be unattended.

**E.22** Remove and properly store all removable media at end of your shift or working day. This also applies to any extended periods of time, i.e., 30 minutes or more, during which workstation will be unattended.

**E.23** Know your Security Manager, IS Security Officer and IS Security Staff. Report security incidents and workstation malfunctions incurred while processing classified data, to IS Security staff representative assigned to your office.

**E.24** Challenge unauthorized personnel and strangers. Do not advise unauthorized persons on microcomputer operations, applications or data in use.

**E.25** Be aware of location of master control switches that secure electrical power to workstations. Label switches to prevent accidental shut-off.

**E.26** All electronic equipment produces emanations which may be monitored at some distance. All workstations used to process classified information must have a Tempest Vulnerability Assessment Request (TVAR) on file. If you do not know TVAR status, contact TASO, ADPSO or Tempest Control Officer before using workstation.

**E.27** Workstation equipped with locking devices are to be locked after close of business for day or when otherwise determined by AIS security staff.

**E.28** Practice good housekeeping, including:

a. Curtail smoking, eating and drinking in immediate vicinity of workstation.

b. Guard against water damage to workstations.

c. Provide adequate fire extinguishers, of a type suitable for use with electronic equipment, as determined by local fire regulations.

d. Operate workstations within manufacturer specified temperature and humidity ranges.

e. Provide adequate lighting and electrical service, including emergency lighting.

f. Routinely clean workstations and surrounding area, including floors, to avoid dust accumulation.

g. Do not store flammable materials in spaces near workstations or magnetic media.

**E.29 REMOTE TERMINALS.** Workstations used as terminals, whether local or remote, to access computer systems, other workstations or networks will be operated with following additional guidelines.

a. Compliance with host system or network requirements, including possible remote terminal agreements. These cover such things as userids, passwords and precautions against unauthorized access.

b. Workstations used as part of a network, local or other, or is connected to another workstation or computer are to be attended while so connected.

c. Incidents of confirmed or possible compromise, unauthorized access or other security violations will be reported to the command responsible for the host system or network, as well as MSC security personnel.

d. Access privileges will be determined by job function and organizational mission.

e. Passwords will not be stored, in any form, on a workstation.

f. Access procedures and workstation capabilities will be treated as Official Use Only and handled on a need-to-know basis.

g. Ensure sign-off is complete before turning the workstation off or leaving it unattended.

h. Secure all terminal operator guides when not in use.

i. Security requirements for terminals are based upon the highest level of information that they can access.

j. Individual workstations connected to an AIS or network processing classified information will be identified to ensure required security control and protection. Identification will be a feature of hardware in combination with operating system.

**E.30 SOFTWARE GUIDELINES FOR MICROCOMPUTERS.** All MSC employees are required to read and comply with license agreements associated with microcomputer software they use.

a. Always keep the license agreement with diskettes and documentation for each program.

b. You may loan software to another MSC employee for management approved purposes, provided the software is used only one machine at a time.

c. You may not copy software except to extent permitted in license agreement (e.g., back-up copies), nor may you copy related documentation.

d. You may load and store software on a fixed (hard) disk provided that license agreement does not prohibit it and stored copy is destroyed should you relinquish control of software.

e. You may load software onto a local area network or transmit it electronically from machine to machine, but only if the license agreement does not prohibit it, and there is a license for each node on the network that uses software.

f. Do not modify software unless permitted by license agreement.

g. If the license agreement does not limit use of the software to a designated (by serial number) machine, you may use program on any machine. However, unless specifically permitted by license, it may not be used on more than one machine at a time.

h. If license agreement or diskette level indicates that a program is licensed only on a designated machine, you must use it only on that machine. All copies (including backup copies) of such software are to be labeled with serial number of designated machine. If you wish to change the designated machine, contact N62.

i. Following activities require prior approval by N2 as they may result in litigation.

(1) Use of software that is covered by a license agreement that states software is confidential or proprietary, or contains trade secret information, or displays a notice or legend to same effect.

(2) Reverse compiling or reverse assembling software.

(3) Use of code from publications such as books or magazines, unless use is specifically granted in publication.

(4) If you want to distribute to other MSC employees a program that you have written, do not include other materials in your distribution unless you have approval. For example, merging operating systems files on a diskette to made a program self-loading and then distributing diskette is prohibited without prior approval.

# APPENDIX F

## RISK ASSESSMENT

**F.1RISK ASSESSMENT PROCEDURE.** Risk Assessments will satisfy requirements of DOD Directive 5200.28 and OPNAVINST 5239.1A. The following procedure will be followed to ensure satisfaction of these instructions. **Contractor assistance will not be utilized without prior written approval from NAVCOMTELCOM as required by paragraph 1.2g of this AISSP.**

a. Step 1. Complete enclosure (4) of DOD Directive 5200.28. This will result in a determination of following factors which are to be addressed in the design, and tested via ST&E.

(1) Minimum user clearance or authorization rating

(2) Maximum data sensitivity rating

(3) Risk index

(4) Minimum security evaluation class for computer-based controls

b. Step 2. If Risk Index is greater than 0, then AIS can not be accredited by COMSC due to DAA requirements of OPNAVINST 5239.1A. In these cases, prior approval of COMSC must be obtained before proceeding with development.

(1) If the Risk Index is 0, then a Method II Risk Assessment, as specified in Appendix E of OPNAVINST 5239.1A will be performed. In such cases, the Risk Assessment may reference this AISSP for any areas covered herein, including the contents of Appendix J. Only parts of Risk Assessment that need be conducted are those that are within the control of the AIS.

(2) If Risk Index is greater than 0, then DAA will be as specified in OPNAVINST 5239.1A. If DAA is not COMSC, then required DAA must be contacted to determine requirements for accreditation. Such systems are not under security control of MSC AIS Security Staff. If DAA remains COMSC, then procedure given for a Risk Index of 0 will be followed.

# APPENDIX G

## SECURITY TEST AND EVALUATION (ST&E)

**G.1 GENERAL.** Security Test and Evaluation (ST&E) is a part of accreditation and certification process. Primary purpose for conducting an ST&E is to obtain technical information to support DAA's decision to accredit or certify an AIS activity or network. ST&E consists of two interrelated phases. First phase determines whether necessary countermeasures have been installed, and the second phase determines whether installed countermeasures are working effectively.

**G.2 SCOPE.** Resources expended for each ST&E and level of detail required will depend upon the level of data being processed and mode of operation. Results of the risk assessment will determine level of detail and scope required for ST&E.

**G.3 POLICY.** As long as COMSC remains the DAA, ST&E is a responsibility of MSC. **Contractor assistance will not be utilized without prior written approval from NAVCOMTELCOM as required by paragraph 1.2g of this AISSP.** It is responsibility of the Project Manager to obtain NAVCOMTELCOM approval for contractor assistance if required.

**G.4 MANDATORY PROCEDURES.** The following general procedures apply to all ST&Es. NAVCOMTELCOM will provide assistance in tailoring the general procedures upon request. Requesting and funding of such assistance is the responsibility of Project Manager, who will coordinate any requests with ADPSO. Requirements of OPNAVINST 5239.1A are to be satisfied for all ST&Es.

a. First step in the ST&E is identifying qualified individuals to perform steps outlined below. If possible, it is preferable for each step to be performed by different individuals. Depending upon the scope of ST&E, each step requires individuals with knowledge of the following:

(1) AIS security

(2) System software/hardware

(3) Application software

(4) Telecommunications

(5) Emanation security

(6) Physical security

(7) Personnel, procedural and administrative security

(8) User/customer functions

b. Second step is reviewing risk assessment for currency and accuracy and identifying and analyzing the nature of threats and vulnerabilities and their respective countermeasures. This provides the basis for development of the ST&E plan.

c. Third step is developing ST&E plan. This plan describes how each countermeasure will be exercised to determine if it is effective. If a "tiger team" will be attempting to defeat system software protection, plan should contain this information. If scenarios, walk-through inspections, documentation and procedure reviews will be utilized, information should be in plan identifying the countermeasures being evaluated by each method. Plan should be modified during actual ST&E if unanticipated situations arise. ST&E plan documentation should address each of the following elements:

(1) Hardware

(2) Software

(3) Physical facility/security

(4) Personnel

(5) Communications

(6) Emanations

(7) Administrative/operating procedures

(8) Data

d. The ST&E plan should include the following items for each element in paragraph G.4c of this appendix:

(1) Test objectives

(2) POA&M for the test

(3) Test team organization

(4) Detailed test plans and procedures

(5) Test data

e. Fourth step is executing ST&E plan. This will be documented as it proceeds, identifying discrepancies and problem areas so that recommendations can be made for inclusion in the report to DAA.

f. The fifth and final step is documenting results of ST&E. This report should include a recommendation to DAA to accredit or not accredit activity or network based upon level of risk identified by ST&E team. If nonaccreditation is recommended, report will contain recommendations regarding security deficiencies.

**G.5 ST&E REPORT.** A sample format for an ST&E report is provided in Figure G-1. Classification of the report is required as specified in paragraph C.2f of Appendix C to this AISSP.

## SAMPLE ST&E REPORT FORMAT

Cover Sheet:

Organization and address

Date of test

Date of report

Classification of report

Index

Executive Summary

Body of Report:

1. AIS Security Environment
    a. Hardware Configuration
    b. Software
    c. Physical Facility/Security
    d. Personnel
    e. Communications
    f. Emanations
    g. Administrative/Operating Procedures
    h. Data
2. Test Objectives
3. Test Results and Analysis
    a. Test results for each area and scenarios used
    b. Overview of general findings and recommendations

FIGURE G-1

c. Specific findings for each area

(1) Summary of problem

(2) Analysis of problem

(3) Alternative solutions

(4) Recommended solutions

(5) Cost to implement, either actual or projected, in terms of dollars or work hours

(6) Impact on system operation

4. Analysis and recommendations regarding test approach and procedures and future system security testing.

5. Proposed POA&M for corrective actions and assignment of responsibilities.

(Attach copy of ST&E Plan)
(Attach copy of Test Team Organization and Members)

# APPENDIX H

## MANDATORY MINIMUM REQUIREMENTS

**H.1 MINIMUM AREAS TO BE ADDRESSED.** Design process for software developed for distribution to MSC activities or other commands will, at a minimum, address following areas. Details will be included in AIS documentation with a summary in an addendum to this AISSP.

a. Access controls, including utilization of user identifications and passwords to verify user identity

b. Application software protection

c. Systems software protection

d. Data file protection

e. Terminal interface protection

f. Communication interface protection

g. Audit trail programs

**H.1.1** MVS System Integrity. All software installed at NCTS by MSC request will support IBM's Statement of MVS System Integrity as set forth in IBM Announcements P81-174, 21 Oct 81 and P80-75, 21 Apr 80. Specifically, such software will not require changes to MVS, or any other currently installed software, where such changes violate MVS System Integrity. IBM Announcement P81-174 contains the following definition for MVS System Integrity - "System Integrity is defined for MVS as the inability of any program not authorized by a mechanism under the customer's control to:

a. circumvent or disable store or fetch protection,

b. access an OS password-protected or a RACF-protected resource (RACF is the Resource Access Control Facility), or

c. obtain control in an authorized state; that is, in supervisor state, with a protection key less than (8), or Authorized Program Facility (APF) authorized."

NCTS may not utilize RACF on any given system, and in such cases above requirements

for RACF will apply to the access control (security) software being used in lieu of RACF.
**H.1.2** Passwords. All MSC systems capable of utilizing password protection will do so. Following guidelines apply:

a. Password length shall be a minimum of six characters.

b. Passwords shall not contain any vowels, and shall contain at least one-non-alphabetic character.

c. Passwords will not contain same character more than twice.

d. Passwords will not be repeated within nine times of their original use.

e. Passwords will not contain keyboard sequences comprised of more than two keys in any direction. (e.g., asd, cde are invalid)

f. Passwords will be classified at highest level of information on the system, but in no case lower than For Official Use Only. Passwords will be treated as Need To Know, and will not be shared.

g. Initial passwords will be assigned in an expired state.

h. Passwords on any system processing information classified SECRET or higher will have a maximum validity period of 30 days. All other passwords will have a maximum validity period of 60 days.

i. Whenever possible, users will be permitted to assign their own passwords.

j. On a given logon attempt, a user will be permitted three attempts to enter the correct password. On the third incorrect entry, the userid will be locked and require intervention by someone with proper authority to unlock userid. In these cases the password will be reset in an expired state. On multiple logon attempts, without the entry of correct password, a total of six incorrect passwords will result in locking userid.

k. Passwords will not be displayed when entered. If a workstation does not permit blanking, then other methods shall be used to ensure that password can not be read when entered.

l. Passwords stored on a system will be encrypted.

m. Passwords printed for distribution will be handled as required for the

appropriate security level. Whenever possible, passwords will be printed on a sealed multipart form in such a way that it is not visible on the top page of form.

n. Lists of passwords will not be maintained.

o. Whenever permitted by the AIS, password entry is to be required only once. The single requirement will be at log-on. All other access will be based on userid.

**H.1.3** Audit Controls. Unless excepted by the ADPSO, all AISs will provide for the following basic audit controls. Microcomputers operating as stand-alone AISs are excepted.

a. Monthly reports to the ADPSO of all security violations, including incorrect passwords and off-hour activity. ADPSSO may alter content and frequency of these reports as deemed necessary for proper audit and control.

b. Automatic logoff of a workstation that is inactive for more than 15 minutes. A 1-minute warning will be provided.

c. Recording of activity other than during scheduled workday (i.e., 0700-1730). This recording need only address log-on attempts as a regular routine, but is to be capable of recording file access if requested.

**H.2 MANDATORY MINIMUM REQUIREMENTS FOR PROCESSING CLASSIFIED OR UNCLASSIFIED SENSITIVE INFORMATION.** In addition to meeting minimum requirements required for all AIS, AIS processing classified or Unclassified Sensitive information will comply with additional requirements specified in section J.3 of Appendix J to OPNAVINST 5239.1A. Safeguards shall be applied so that Classified and Unclassified Sensitive information is accessed only by authorized persons, is used only for its intended purpose, retains its content integrity and is marked properly as required. Documentation for satisfying these requirements will be provided via ST&E documentation and an addendum to this AISSP.

**H.4 MANDATORY MINIMUM REQUIREMENTS FOR NETWORKS.** In addition to meeting the minimum requirements in paragraphs H.1 and H.2, all MSC networks will comply with the following. Satisfaction of these requirements will be documented in the ST&E.

a. Classification level of network will be at highest level of information processed by any node[1]. This requirement applies regardless of whether or not node processes classified information when logged on network. If a node has a connection of any type to network at any time, then classification level of that node will be used in determining classification level of the network.

b. If network processes classified information then network, including all cables, will satisfy the requirements for emanation control (TEMPEST) as required by OPNAVINST C5510.93E.

c. An AIS Network Security Officer will be appointed as required by Chapter 2 of the AISSP.

d. Networks have a lower limit than AISs at which the DAA moves from COMSC to NAVCOMTELCOM. These limits are given in Figures 3-2 and 3-3 of OPNAVINST 5239.1A. Networks requiring other than COMSC as DAA are not to be implemented without prior approval from COMSC.

e. Networks installed and operated by MSC will be restricted to MSC controlled spaces unless prior approval is granted by COMSC. Networks installed and operated by MSC will be limited to interconnection of MSC accredited AISs as specified in A.1 of enclosure (5) to DOD Directive 5200.28.

---

1- A **node** as used in this context is defined to mean any equipment of any form that is a part of network. This definition is purposely different from the usual definition of a node in a network.

# APPENDIX I

## ACCREDITATION SUPPORT DOCUMENTATION

**I.1 DOCUMENTATION REQUIREMENTS.** Accreditation Support Documentation provides information to support request for accreditation. It offers evidence that AIS activity or system has effectively implemented appropriate countermeasures consistent with protection requirements for data level and security mode of operation to be authorized. The documentation is to include the following items.

NOTE: The below requirements are taken directly from OPNAVINST 5239.1A. In some cases a strict application of the requirements would result in an large volume of data with little real value. For example, providing drawings showing the location of all workstations and the specific equipment at each location. Upon request, ADPSO will review requirements of this appendix as they apply to a specific case and may grant a reduction in these requirements.

a. Name, position and telephone number of the ADPSO and ADPSO who will serve as a primary point of contact for the accreditation. For projects, the ADPSSO is the primary point of contact.

b. Identification and location of all AIS equipment, e.g., mainframe components, on-line peripherals, peripheral processors, communications processors, encryption devices, remote terminals and devices, network interfaces, workstations, etc. Provide charts, engineering drawings, etc.

c. Line diagrams showing interconnection of AIS equipment, communications lines and protection of lines.

d. Approximate percentage of each application category of data to be processed (identified by project or task) versus level of data (Classified, Unclassified Sensitive or Unclassified) and the type within each level (Secret, Confidential, personal, financial, etc.)

e. Information briefly describing the operating system and applications software (vendor acronyms may be used for industry-wide software) for AIS systems and communications and network dependent applications software for networks, if applicable.

f. Current and proposed security modes of operation.

g. Copy of AIS Security Operating Procedures and other applicable command security directives, security incident handling procedures, operating procedures, AIS product marking and distribution procedures, procedures for control of modification to operating and application software, etc.

h. Risk assessment documentation.

i. Description of all countermeasures.

j. Copies of previous system and/or network accreditations and interim authorities to operate.

k. Certification of compliance with security directives.

l. ST&E test plans.

m. ST&E test reports.

n. Tempest accreditation, if applicable.

o. Physical accreditation, if applicable.

p. Contingency Plan.

q. Contingency Plan test results.

r. MSC or Project AIS Security Plan, as applicable.

s. Other documentation as required by the ADPSO.

**I.2 ACTIVITY ACCREDITATION SCHEDULE (AAS).** This planning form, promulgated in OPNAVINST 5239.1A, is to be used to track accreditation process. AAS is provided in Figure I-1. Include AAS with other accreditation support documentation.

**I.3 DOCUMENTATION REVIEW AND RECOMMENDATION.** ADPSO and other personnel appointed by DAA will review accreditation support documentation. Based upon this review, ADPSO will request any required changes or enhancements prior to submitting request for accreditation to DAA. To ensure an unbiased review, reviewers are not to have personal and direct involvement in preparing documentation. ADPSO is responsible for packaging and submitting request for accreditation to DAA. This request will include ADPSO recommendation for or against accreditation.

NOTE: It is recognized that ADPSO is responsible for preparing and submitting accreditation support documentation for MSC at an overall activity level. In this capacity it is not possible for ADPSO to be removed from documentation preparation related to MSC at activity level.

## ACTIVITY ACCREDITATION SCHEDULE

LEGEND EXPLANATION

1. UIC - Unit Identification Code. The UIC for MSC Headquarters is 00033.
2. DAA - Designated Approving Authority - Commander, Military Sealift Command.
3. Level of processed data -
    a. Classified
    b. Unclassified, sensitive
    c. Other unclassified
4. Modes of operation - System high, dedicated, controlled, multilevel.
5. AIS element information
    a. Application name (e.g., payroll, logistics, finance, etc.)
    b. Hardware (CPU) manufacturer (e.g., IBM 3090, Univac 1160, etc.)
    c. Software (operating system) (e.g., Univac (Exec 1100))
    d. Facility, building number/room number
    e. Communications - Number of nodes (locations) and number of terminals
    f. Networks (e.g., AUTODIN interface, TELENET, ARPANET)
    g. TEMPEST required: yes or no; if yes, provide TEMPEST task number
    h. Is Communication Security (COMSEC) required? (yes or no)
    i. Is Data Encryption (DES) required? (yes or no)
6. Estimated schedule for completing accreditation:
    a. Risk Assessment: estimated start/completion dates

FIGURE I-1

b. ST&E: plan development date; test date

c. Contingency Plan development date

d. Date for submitting request for Certification

7. Name of Automated IS Security Officer (ADPSO)

# APPENDIX J

## PROJECT ACCREDITATION AND CERTIFICATION

Each MSC software and hardware project requires either accreditation or certification. Each project will build upon the base provided in AISSP. An addendum will be provided for AISSP covering specifics of project not addressed in AISSP. These addenda will become part of this Appendix.